Vysoká škola báňská – Technická univerzita Ostrava
Ekonomická fakulta

KATEDRA APLIKOVANÉ INFORMATIKY

Audit bezpečnosti informací v nadnárodní společnosti

Information security audit in a multinational company

Student: Magda Vašínková

Vedoucí bakalářské práce: Ing. Jiřina Petříková

Ostrava 2011

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání bakalářské práce

Student: **Magda Vašínková**

Studijní program: B6209 Systémové inženýrství a informatika

Studijní obor: 6209R001 Aplikovaná informatika

Téma: Audit bezpečnosti informací v nadnárodní společnosti
Information Security Audit in a Multinational Company

Zásady pro vypracování:

1. Úvod
2. Metodická východiska a nástroje
3. Analýza současného stavu ve společnosti
4. Příprava auditu
5. Provedení auditu
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků bakalářské práce
Přílohy

Seznam doporučené odborné literatury:

ARNASON, S. T.; WILLETT, K. D. *How to Achieve 27001 Certification - An Example of Applied Compliance Management.* 1st ed. New York: Auerbach Publications, 2007. 352 s. ISBN 978-0849336485.
DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* 1. vyd. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.
KOPÁČIK, I. a kol. *Riadenie a audit v informačnej bezpečnosti.* 1. vyd. Bratislava: TATE International Slovakia, 2007. 322 s. ISBN 978-80-969747-0-2.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Jiřina Petříková**

Datum zadání: 26.11.2010
Datum odevzdání: 11.05.2011

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * OSTRAVA * Ekonomická fakulta 1

Ing. Jan Ministr, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

„Místopřísežně prohlašuji, že jsem celou práci včetně všech příloh vypracovala samostatně."

9. května 2011 Magda Vašíčková .....

Obsah

1. Úvod ... 1

2. Metodická východiska a nástroje ... 2

2.1 Pojmy ... 2

2.1.1 Bezpečnost informací ... 2

2.1.2 Audit ... 4

2.2 Historie auditu ... 7

2.3 Normy ISO/IEC ... 7

3. Analýza současného stavu ve společnosti ... 11

3.1 Bezpečnostní politika společnosti ... 12

3.2 Hardwarová struktura závodu ... 12

3.3 Softwarová struktura závodu ... 13

3.4 Klasifikace dat ... 13

3.4.1 Veřejné ... 14

3.4.2 Vnitřní ... 14

3.4.3 Důvěrné ... 14

3.5 Uživatelské účty a řízení přístupu ... 15

3.6 Hesla ... 16

3.7 Antivirová ochrana ... 17

3.8 Archivace dat ... 17

3.9 Skartace dat ... 18

3.10 Definice rolí a povinností v oblasti informační bezpečnosti ... 18

3.10.1 Ředitel bezpečnosti ve společnosti ... 18

3.10.2 Manažer informační bezpečnosti ... 18

3.10.3 Regionální manažer informační bezpečnosti ... 19

3.10.4 Lokální manažer informační bezpečnosti ... 19

3.11 Lidské zdroje 19
3.11.1 Dohody o důvěrnosti 19
3.12 Zabezpečení závodu 19
3.13 Krizový plán 20
4. Příprava auditu 21
4.1 Cíl auditu 21
4.2 Plán auditu 21
4.3 Hodnocení auditu 22
5. Provedení auditu 23
5.1 Výsledek auditu 47
6. Závěr 49
Seznam použité literatury 50
Seznam zkratek 51
Prohlášení o využití výsledků bakalářské práce 52
Seznam příloh 53

1. Úvod

Lidský druh se prosadil díky své vynalézavosti a touze získávat nové znalosti. S příchodem doby moderních technologií, zejména internetu, se zvyšuje potřeba ochránit si tyto znalosti v podobě informací nebo know-how.

Proto se stává informační bezpečnost nedílnou součástí našeho každodenního života, ať už v osobním životě, kdy se snažíme si ochránit své soukromí a citlivé údaje, tak zejména v pracovním životě. V podnikatelské sféře je díky útokům, sabotážím nebo i pouhé neinformovanosti zaměstnanců každodenně ohrožena konkurenceschopnost podniku či dobré jméno firmy. U státní sféry jsou pak ohrožena osobní data o všech fyzických a právnických osobách vyskytujících se na území daného státu a samozřejmě i státní tajemství.

Cílem informační bezpečnosti je snížení rizika odhalení informací, změny nebo zničení klíčových obchodních dat na přijatelnou úroveň. Výsledkem je soubor vzniklých norem a zákonů obsahující bezpečnostní požadavky, které by měly jednotlivé subjekty splňovat a tím bránit únikům důležitých aktiv společnosti.

Účelem této práce je zjistit pomocí auditu stav ochrany informací v nadnárodní společnosti a upozornit na oblasti, které jsou nedostatečně chráněny. Z důvodu zkoumání citlivé oblasti podniku nebude v této práci použito jméno společnosti. Dále budou některé údaje o firmě upraveny a o společnosti se v práci budu zmiňovat jako o ABC spol. s r.o.

Nejprve práce předloží teoretická východiska, tedy vysvětlení základních pojmů z oblasti bezpečnosti informací a auditu. Následovat bude popis základních kamenů tohoto oboru, kterými jsou normy ISO a certifikace.

V druhé části bude práce obsahovat analýzu současného stavu informační bezpečnosti organizace ABC spol. s r.o. V této části budou popsána bezpečnostní opatření, zavedená ve zkoumané společnosti, která jsou v současné době ošetřena systémem směrnic.

Ve třetí části se bude práce věnovat přípravě auditu. Bude zvolena norma, kterou se bude audit řídit, sestaven plán auditu a způsob hodnocení, který bude použit.

Čtvrtá část bude obsahovat provedení samotného auditu bezpečnosti informací dle sestaveného plánu a navržení případných doporučení pro zlepšení úrovně zabezpečení na odpovídající úroveň.

Cílem této bakalářské práce je provést analýzu současného stavu, audit a zhodnocení stavu systému řízení informační bezpečnosti ve zvolené společnosti. Závěr práce zhodnotí celý průběh auditu.

2. Metodická východiska a nástroje

2.1 Pojmy

2.1.1 Bezpečnost informací

Aktiva

Mezi aktiva organizace můžeme zahrnout:

- fyzická aktiva (např. počítačový hardware, komunikační prostředky);
- informace/data (např. dokumenty, databáze);
- software;
- schopnost vytvářet určité produkty a poskytovat služby (know-how);
- lidi a
- nehmotné hodnoty (např. image).

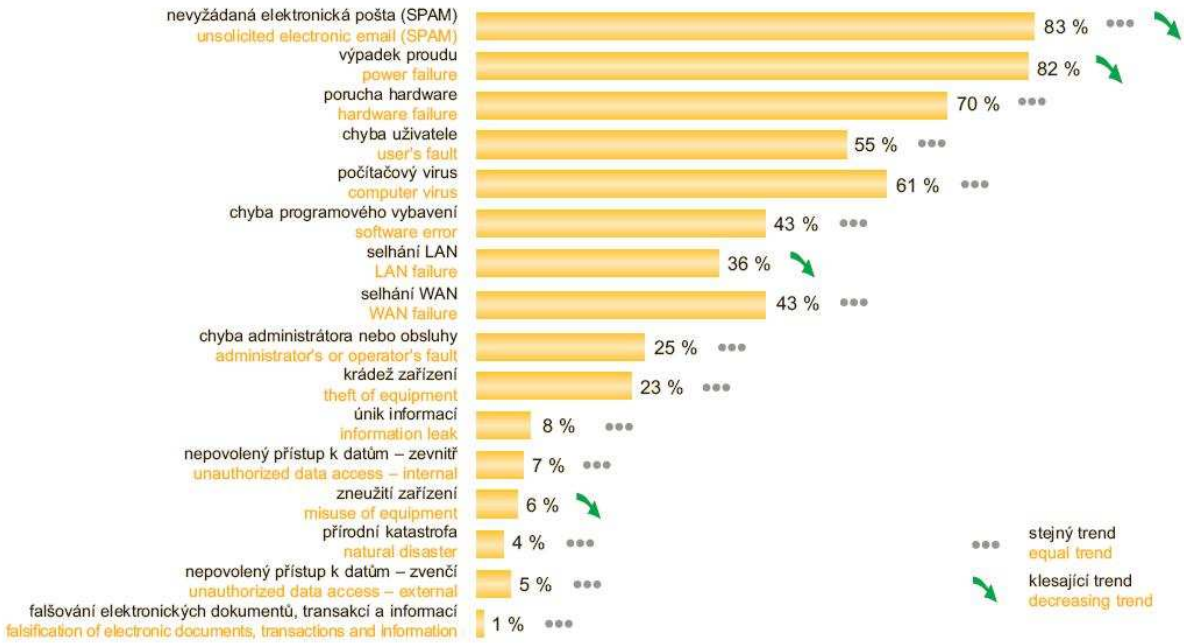
Jedním z požadavků informační bezpečnosti je právě evidence všech těchto důležitých aktiv spojených s informačními systémy. Do tohoto seznamu by měla být zahrnuta všechna aktiva, která mají pro organizaci cenu a díky této ceně si zaslouží určitý stupeň ochrany.

Hrozby

Hrozbou rozumíme subjekty nebo události, jež za využití zranitelnosti aktiv způsobí nežádoucí incident a tím mohou způsobit škodu majetku organizace. Subjekt je osoba nebo zařízení. Škoda se může vyskytnout jako důsledek přímého nebo nepřímého útoku na aktiva.

Hrozby mohou být přírodního (např. zemětřesení, blesk, povodeň či požár) nebo lidského charakteru. U jiného dělení se setkáváme s hrozbami úmyslnými (např. odposlech, změna informace, krádež, atp.) nebo náhodnými (např. chyby, opomenutí, fyzické nehody, atp.).[8]

Nejčastěji se vyskytující hrozby, které firmy zaznamenávají, jsou zobrazeny v grafu 2.1, který je sestaven z výsledků každoročně prováděného průzkumu za účasti Národního bezpečnostního úřadu, společnosti Ernst&Young a nakladatelství Data Security Management.



Graf 2.1. Výskyt bezpečnostních hrozeb za roky 2008 a 2009, Zdroj: Průzkum informační bezpečnosti v ČR 2009

Zranitelná místa

Dalším termínem pro „zranitelná místa“ může být „zranitelnost“. Oba vyjadřují ta slabá místa aktiv, která mohou být využita hrozbou ke způsobení škody nebo ztráty. Tato zranitelná místa umožňují hrozbám ovlivnění aktiv, avšak sama o sobě nejsou nutně příčinou škody. Zranitelnost může být u některých druhů aktiv vlastní a k jejímu odstranění dojde až po změně typu aktiva. V takovýchto případech by měla být aktiva monitorována. Dynamické změny v prostředí mohou způsobovat i změny hrozeb a tím i změnu zranitelných míst.

Analýza zranitelnosti prozkoumává tato slabá místa aktiv, která mohou být využita identifikovanými hrozbami. Při analýze se berou na vědomí jak vlivy prostředí, tak již zavedená ochranná opatření. Výsledkem je zhodnocení, jak snadno lze dosáhnout poškození konkrétního aktiva hrozbou.

Dopad

Důsledkem realizace náhodné nebo úmyslné hrozby je dopad. Následkem vlivu bezpečnostního incidentu na aktiva může být buď úplné zničení, poškození informačního systému, nebo narušení bezpečnosti informací. Součástí dopadu jsou i nepřímé následky jako poškození důvěry ve společnost nebo ztráta tržního podílu.[8]

Výpočet dopadu na chod podniku je proces, kterým se určuje vliv incidentu na obchodní operace a strategické schopnosti podniku. Nejčastěji je dopad prezentován stanovením finančních nákladů v případě ztráty či poškození konkrétního aktiva. Další z možností je stanovení empirické stupnice síly (např. 1 až 10) nebo použití adjektiv

(například nízký, střední, vysoký). Důvodem tohoto měření je vytvoření rovnováhy mezi výsledky nežádoucích incidentů a náklady na ochranná opatření.

porucha hardware hardware failure	152 000 Kč
výpadek proudu power failurer	123 000 Kč
počítačový virus computer virus	108 000 Kč
nevyžádaná elektronická pošta (SPAM) unsolicited electronic email (SPAM)	86 000 Kč
selhání WAN WAN failure	74 000 Kč
selhání LAN LAN failure	39 000 Kč
chyba programového vybavení software error	20 000 Kč

Tabulka 2.2 Průměrné přímé finanční dopady nejzávažnějších bezpečnostních incidentů, Zdroj: Průzkum informační bezpečnosti v ČR 2009

Riziko

Rizikem rozumíme potenciální možnost, že daná hrozba využije zranitelnosti. Výsledkem je ztráta nebo poškození aktiv organizace. Hrozba za využití zranitelnosti může znamenat riziko i pro více aktiv současně.

Základními prvky pro určení míry rizik jsou pravděpodobnost výskytu ohrožujícího incidentu, velikost jeho dopadu a zranitelnost ohroženého aktiva, přičemž změna kteréhokoliv prvku v tomto řetězci (aktiva, hrozby, zranitelnosti nebo ochranných opatření) může znamenat i změnu míry rizika.[8]

Bezpečnostní politika

Hlavním cílem bezpečnostní politiky společnosti je zajištění dostupnosti, důvěrnosti a integrity informací, které jsou zpracovávány ve firemním prostředí, a zajištění odpovědnosti zaměstnance za jeho činnost v tomto prostředí. Za tím účelem je zpracován registr rizik, který obsahuje úplnou identifikaci všech informačních aktiv společnosti, jejich klasifikaci, identifikaci hrozeb a stanovení úrovně rizika. V registru jsou stanovena opatření, která snižují úroveň rizika na akceptovatelnou hranici.

Koncepce bezpečnosti informací vychází ze zásady používání údajů a informací pouze tam, kde je jich nezbytně zapotřebí. Chráněná aktiva smí používat pouze ty osoby, které je potřebují ku prospěchu společnosti nebo v souladu s jejími zájmy, a to s takovými oprávněními, která jsou zapotřebí.[3]

2.1.2 Audit

Audit je systematický, nezávislý a dokumentovaný proces získávání důkazů z auditu a jeho objektivního hodnocení s cílem stanovit rozsah splnění kritérií auditu. [dle ISO 19011]

Audit systému řízení se vykonává principem náhodné kontroly vybraných prvků informační bezpečnosti při přezkoumání důkazů auditu určených na základě zavedené a používané normy.

Dle pravidel je povoleno, aby klient požádal o odůvodněné neuplatňování některého ze článků dané normy.

Rozsah a hranice systému řízení informační bezpečnosti definuje předmět auditu. Zde se stanoví působnost, charakteristika podnikání organizace, aktiv, technologií a lokality. Předmět auditu obsahuje taktéž zdůvodnění vyžádaných výjimek z rozsahu působnosti systému řízení informační bezpečnosti.

Auditor

Jako auditor vystupuje osoba s prokázanými osobními vlastnostmi a kompetentností vykonávat audit systému řízení. Zkoumá profesionálně a nezávisle shodu kritérií auditu s prvky normy.

V rámci auditu se můžeme setkat i s týmem auditorů, který je veden vedoucím auditorem. Ten je zodpovědný za naplánování termínu auditu, za přezkoumání dokumentace systému řízení informační bezpečnosti, nerušený průběh a ukončení auditu. Týmem auditorů pak rozumíme skupinu odborných auditorů uzpůsobilých k vykonávání auditu, kteří pod vedením vedoucího auditora vykonávají audit u klienta na místě. Součástí týmu auditorů může být i technický expert jako specialista kvalifikovaný pro stanovenou oblast auditu, který však sám činnost auditora nevykonává. Jeho odbornost a výsledky jeho práce (např. měření, analýzy, testy, atp.) jsou využívány auditory pro stanovení a podporu jejich zjištění vyplývajících z auditu. Vedoucího auditora a jeho tým jmenuje vedoucí certifikačního orgánu.

Klient auditu

Osoba, resp. organizace, která požaduje provedení auditu. Může se jednat o zástupce vedení společnosti, resp. klientem může být i zákaznická organizace (v případě, že se jedná o audit u dodavatele). Určuje cíl(e) auditu, rozsah a kritéria auditu.[9]

Osoba odpovědná za zorganizování auditu

Osoba, která má vymezenu odpovědnost za řízení programu auditů. V řadě případů je totožná s klientem auditu. Může se jednat o představitele managementu pro kvalitu, resp. zástupce vedení společnosti.

Mezi povinnosti odpovědné osoby patří: stanovení cílů jednotlivých auditů, které ve firmě probíhají, zajištění zdrojů potřebných pro vykonání auditů, zajištění uplatňování programu auditů, povinnost zajistit odpovídající záznamy a dále monitorování, přezkoumání

a zlepšování programu auditů. Jmenuje vedoucího auditora a spolupracuje s ním na sestavení týmu auditorů.

Auditovaný

Osoba, resp. oddělení, u které, resp. ve kterém probíhá audit. Jeho povinností je poskytnout přístup k informacím a datům, která si auditor v průběhu auditu vyžádá (rozsah informací a údajů může být omezen rozhodnutím vedení společnosti, resp. může vyplynout z dané funkce - např. přístup do osobních složek zaměstnanců, smlouvy s významnými klienty, atp.) a odpovídá auditorovi na položené dotazy, předkládá další důkazy potřebné pro provedení auditu.

Důkaz z auditu

Záznam nebo konstatování informace, které souvisí se skutečnou situací a má prokázat naplnění kritérií auditu; musí být ověřitelné; důkaz z auditu může být kvalitativní nebo kvantitativní.

Kritéria auditu

Soubor politik, postupů nebo požadavků; jsou považována za základ, se kterým se porovnávají důkazy z auditu (např. požadavky normy ISO 9001).

Závěr z auditu

Výstup z auditu. Tuto zprávu zpracovává vedoucí auditor na základě důkazů získaných v průběhu auditu jednotlivými auditory. Zpráva by měla obsahovat vyjádření k naplnění cílů auditu.

Zjištění z auditu

Výsledky hodnocení shromážděných důkazů z auditu dle kritérií auditu; označují shodu, neshodu vůči kritériím, resp. příležitost ke zlepšování.

Program auditů

Soubor auditů (může se jednat i o jeden audit) naplánovaných na určitý časový rámec. Program auditů zahrnuje všechny činnosti nezbytné k plánování, organizování a provádění auditů v daném období.

Plán auditu

Popis činností a uspořádání postupu auditu (týká se 1 konkrétního auditu).[9]

Certifikační orgán

Organizace, které vydávají pověření třetím stranám; umožňující těmto stranám provádět příslušné testování a audit společností, jež mají zájem o obdržení certifikátu dané normy.

2.2 Historie auditu

Původ auditu můžeme nalézt ve starověkém Egyptě, kde bylo požadováno, aby o příjmech referovali dva nezávislí úředníci. Římští vládci ve třetím století př. n. l. určovali tzv. kvestory, kteří kontrolovali evidenci ve všech provinciích. Kvestoři byli povinni skládat zprávy před shromážděním posluchačů[1]. Z tohoto období tedy nejspíše pochází slovo audit.[5]

Audit IS a bezpečnosti má v celosvětovém měřítku za sebou již dlouhou cestu od svých raných počátků. Na konci 70. let minulého století vzniká v USA asociace auditorů elektronického zpracování dat (tzv. Electronic Data Processing Auditors Association) v důsledku nárůstu užívání technologií v účetních systémech a potřeby kontrolovat dopad informačních technologií na výsledky kontrolních služeb. Pro tuto dobu bylo charakteristické, že se tento druh auditu chápal spíše jako „umění", nebyl zformulován do vědní disciplíny, neměl své nástroje, atd. Druhou fázi vývoje zaznamenáváme v 80. letech 20. století, kdy se v USA objevuje systémový audit a z auditu IS se stala inženýrská disciplína. Zároveň dochází k transformaci Asociace EDP auditů do organizace ISACA (Information Systems Audit and Control Association), která působí dodnes jako největší mezinárodní organizace sdružující auditory informačních systémů. Následně od 90. let 20. století se setkáváme přímo s pojmem audit bezpečnosti informací. [7]

2.3 Normy ISO/IEC

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém pro celosvětovou standardizaci. Národní orgány, které jsou členy ISO nebo IEC se zúčastňují na vývoji mezinárodních norem prostřednictvím technických komisí. Tyto komise jsou ustanoveny organizacemi pro jednotlivé oblasti technické činnosti. Technické komise ISO a IEC vzájemně spolupracují a spolupracují s nimi i jiné mezinárodní vládní nebo nevládní organizace. V oblasti informačních technologií ISO a IEC byla založena společná technická komise ISO/IEC JTC 1. [6]

Série standardů ISO 2700x je rezervovaná pro oblast informační bezpečnosti. Zde je přehled několika nejdůležitějších platných norem:

ISO/IEC 27000:2009 Information technology - Security techniques – Information security management systems – Overview and vocabulary

Obsahuje definice terminologie a slovník pojmů používaných v dalších standardech této série.

[1] z lat. audire = poslouchat

ISO/IEC 27001:2005 (BS 7799-2) Information technology - Security techniques - Information security management systems - Requirements

Norma poskytuje model pro zavedení a správu efektivního systému řízení bezpečnosti informací (ISMS). Dále stanovuje jednoznačné požadavky na systém řízení a díky tomu umožňuje kontrolu zavedení ISMS a případnou certifikaci, tedy nezávislé ověření ISMS třetím (důvěryhodným a akreditovaným) subjektem.[11]

ISO/IEC 27002:2005 (dříve ISO/IEC 17799:2005) Information technology - Security techniques - Code of practice for information security management

Toto nové vydání mezinárodní normy obsahuje více než 133 strukturovaných oblastí doporučení rozdělených do 11 kapitol, ve kterých je obsaženo více než 5000 přímých a odvozených bezpečnostních opatření, podporujících dosahování podnikatelských cílů, přičemž odpovědnost za ně je možné jednoduše přiřadit osobám s odpovídajícími funkcemi. Tím umožňuje zjistit velmi rychle stav bezpečnosti informačního systému organizace a zároveň vytvořit východiska pro jeho zlepšení, zejména vymezením oblastí, které nejsou dostatečně zajištěny.

ISO/IEC 27003:2010 Information technology - Security techniques -- Information security management system implementation guidance

Zaměřuje se na kritické aspekty potřebné pro úspěšné plánování a realizaci systému řízení bezpečnosti informací podle normy ISO/IEC 27001:2005. Popisuje proces specifikace ISMS a design od počátku až po zavádění plánů. Obsahuje popis procesu od získání souhlasu vedení až k implementaci ISMS, definuje projekt implementace ISMS (podle ISO/IEC 27003:2010 jako projekt ISMS) a poskytuje návod, jak plánovat projekt ISMS.

ISO/IEC 27004:2009 Information technology - Security techniques -- Information security management – Measurement

Obsahuje pokyny pro rozvoj a využití opatření a měření s cílem posoudit účinnost implementovaného systému řízení bezpečnosti informací (ISMS).

ISO/IEC 27005:2008 Information technology - Security techniques -- Information security risk management

Pokyny pro řízení rizik bezpečnosti informací, které podporují obecné pojmy uvedené v ISO/IEC 27001 a jsou určeny k asistenci během implementace informační bezpečnosti založené na přístupu k řízení rizik.[10]

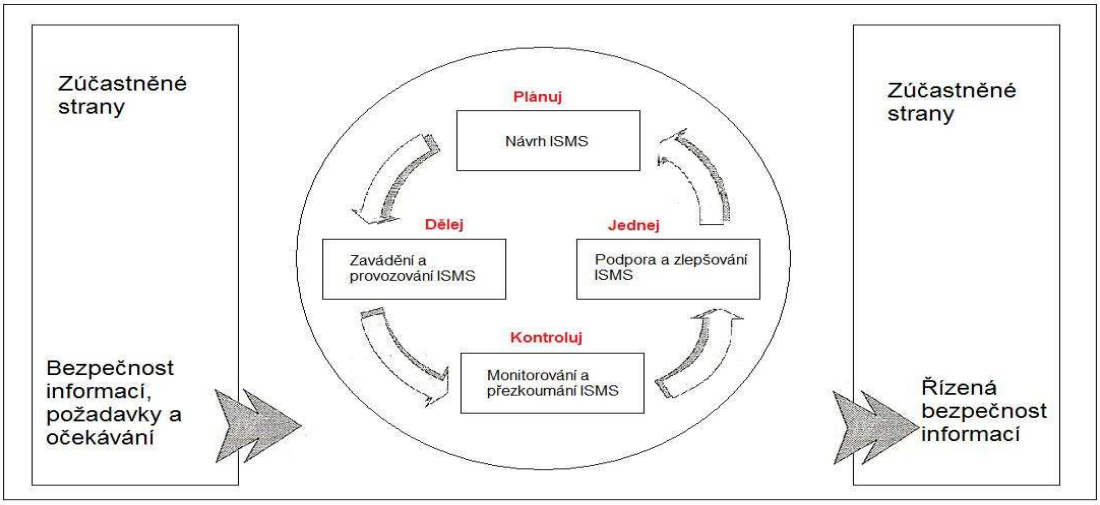
Systém managementu informační bezpečnosti

Systém managementu informační bezpečnosti (ISMS) poskytuje rámec pro efektivnější a přehlednější řízení bezpečnostních procesů v každé organizaci. Poskytuje nástroje, které umožňují vědomě rozhodovat o bezpečnostních problémech a rizicích a vynakládat efektivně přiměřené prostředky do této oblasti. Cílem ISMS není dosáhnout bezpečného informačního systému, ale trvale udržovat bezpečnost informací na úrovni, která uspokojuje potřeby a požadavky organizace. V tomto smyslu je třeba chápat i certifikáty ISMS podle ISO/IEC 27001:2005 vydané akreditačními společnostmi. Tento certifikát nepotvrzuje, že má daná organizace bezpečný informační systém, ale že proces budování, provozu, monitorování a zlepšování informační bezpečnosti je řízený vhodným způsobem.[6]

Mezinárodní norma ISO/IEC 27001:2005 přijala model známý jako „Plánuj-Dělej-Kontroluj-Jednej“ (Plan-Do-Check-Act neboli PDCA), který může být aplikován na všechny procesy ISMS. Obrázek 2.3 zobrazuje, jak ISMS přijímá požadavky bezpečnosti informací a očekávání zainteresovaných stran jako vstup a jak pomocí nezbytných činností a procesů zajišťuje bezpečnost informací jako výstup splňující tyto požadavky a očekávání.

Model PDCA popisuje životní cyklus systému řízení. Jeho základem je procesní přístup k řízené oblasti. Při implementaci modelu PDCA je všeobecně potřebné zvážit minimálně tyto skutečnosti:

- pochopení požadavků na oblast a stanovení zásad, které mají být dodrženy;
- zavedení a provedení opatření v souladu se systémem managementu organizace jako takovým;
- monitorování a přehodnocování funkčnosti opatření;
- neustálé zlepšování podporované systémem managementu.



Graf 2.3. Znázornění modelu PDCA v ISMS, Zdroj: Norma ISO/IEC 27001:2005

Plánuj – plánování představuje základ budování systému řízení informační bezpečnosti. Je stanoven rozsah systému řízení bezpečnosti, je definována bezpečnostní politika, je navrhnuto řízení rizik, včetně jejich vyhodnocení a jsou vybrána opatření pro snížení rizik.

Dělej – fáze „Dělej“ zahrnuje zavedení a využívání bezpečnostních opatření, procesů a postupů, včetně monitorování jejich účinnosti.

Kontroluj – v této fázi je posouzena funkčnost a efektivnost procesů a opatření, jsou vykonány interní audity, přehodnocena rizika a je přezkoumán systém řízení bezpečnosti informací.

Jednej – na základě výsledků předcházející fáze jsou vykonána nápravná a preventivní opatření.

Definice politiky ISMS je klíčový strategický dokument, který definuje rámec pro stanovení cílů, směrnic a principy informační bezpečnosti ve společnosti.

Řízení informačních rizik se zakládá na efektivním principu řízení rizik působících na informační systém (IS). Důležitým vstupním předpokladem je analýza těchto rizik a jejich ohodnocení (jsou brány v potaz jak rizika dopadu na celou společnost, tak pravděpodobnost selhání bezpečnostních opatření a úroveň rizika), které poskytuje možnosti pro rozhodování o jejich řízení.

Samotná identifikace rizik je prováděna následovně:

- identifikace aktiv a jejich vlastníků;
- identifikace hrozeb pro tyto aktiva;
- identifikace zranitelností;
- identifikace dopadů. [6]

Podle průzkumu Národního bezpečnostního úřadu však stále 45% společností spoléhá při řízení informační bezpečnosti na interně vyvinuté standardy, ať již na lokální, či celopodnikové úrovni.

3. Analýza současného stavu ve společnosti

Společnost ABC spol. s r.o. působí na poli automobilového průmyslu již 140 let, kdy byla založena v Německu. V současné době patří mezi největší dodavatele v této oblasti. Společnost dnes zaměstnává přibližně 150.000 zaměstnanců v téměř 200 lokalitách po celém světě. Jako dodavatel produktů v oblasti pneumatik, brzdových systémů, podvozkových komponentů a vozidlové elektroniky přispívá společnost ke zdokonalování jízdní bezpečnosti a ochraně globálního klimatu. Společnost používá celosvětové aplikace a komunikační sítě pro uchování a výměnu informací.

V rámci tohoto koncernu bylo vytvořeno oddělení s názvem InfoSec, jehož náplní je právě řízení a koordinování informační bezpečnosti v rámci celé společnosti. Hlavní sídlo se nachází v Německu.

Závod, pro který je tento audit vytvořen, se nachází ve Frenštátu pod Radhoštěm. Všechny poznatky o společnosti jsou získány právě z tohoto prostředí.

Od prosince roku 1999 je závod zapsán v obchodním rejstříku. ABC spol. s r.o. v tomto závodu zaměstnává více jak 2.000 osob pracujících ve středisku o rozloze 40.000 m^2. Pobočka byla již v minulosti certifikována těmito standarty: ISO 9001[1], VDA 6.1[2] a dle ISO 14001:1996, ISO/TS 16949:2002[3].

Infrastrukturu informačních technologií řídí lokální středisko IT, jež je rozděleno do 4 týmů:

- IT1 – infrastruktura závodu
- IT2 – organizace závodu
- IT3 – UNIX systémy
- IT4 – podpora SAP

Manažer tohoto IT oddělení je současně i zodpovědnou osobou za bezpečnost informací v závodu. Tímto je přímo podřízen řediteli závodu, který jej jmenuje.

[1] Certifikace systému managementu kvality.
[2] Německá certifikace systému managementu kvality pro automobilový průmysl.
[3] Certifikace systému managementu jakosti.

3.1 Bezpečnostní politika společnosti

Bezpečnostní politika společnosti ABC spol. s r.o. je v současné době ošetřena systémem směrnic a nařízeními. Tyto platí pro všechny závody. Politika bezpečnosti informací i směrnice jsou vytvářeny tak, aby splňovaly mezinárodní normu ISO/IEC 27001:2005 a v letošním roce je naplánováno další přiblížení k této certifikaci.

Bezpečnostní politika byla vydána správní radou, reprezentovanou členem rady zodpovědným za lidské zdroje. Dále je radou jmenován zaměstnanec řídící bezpečnost, tzv. CSO, jehož pravomocí je řízení všech otázek bezpečnosti informací.

Hlavní dokument seskupující jednotlivé oblasti vstoupil v platnost 1. 2. 2001 a od té doby je nezměněn. Společnost vymezuje tyto hrozby týkající se bezpečnosti informací:

- penetrace - propustnost zabezpečení informačních systémů před vnějším zásahem, útoky neoprávněnými osobami nebo systémy;
- zneužití - úmyslné nebo neúmyslné použití informačních aktiv pro jiné než povolené účely;
- neoprávněné smazání nebo neúmyslné poškození informačních aktiv vlivem porušení integrity nebo důvěrnosti obchodních funkcí a informací, modifikace nebo zveřejnění informací;
- zkreslení - útoky neoprávněnými osobami nebo systémy, které se vydávají za legitimní uživatele nebo systémy;
- selhání komponenty - deaktivace bezpečnostních mechanismů poruchou informačních systémů.

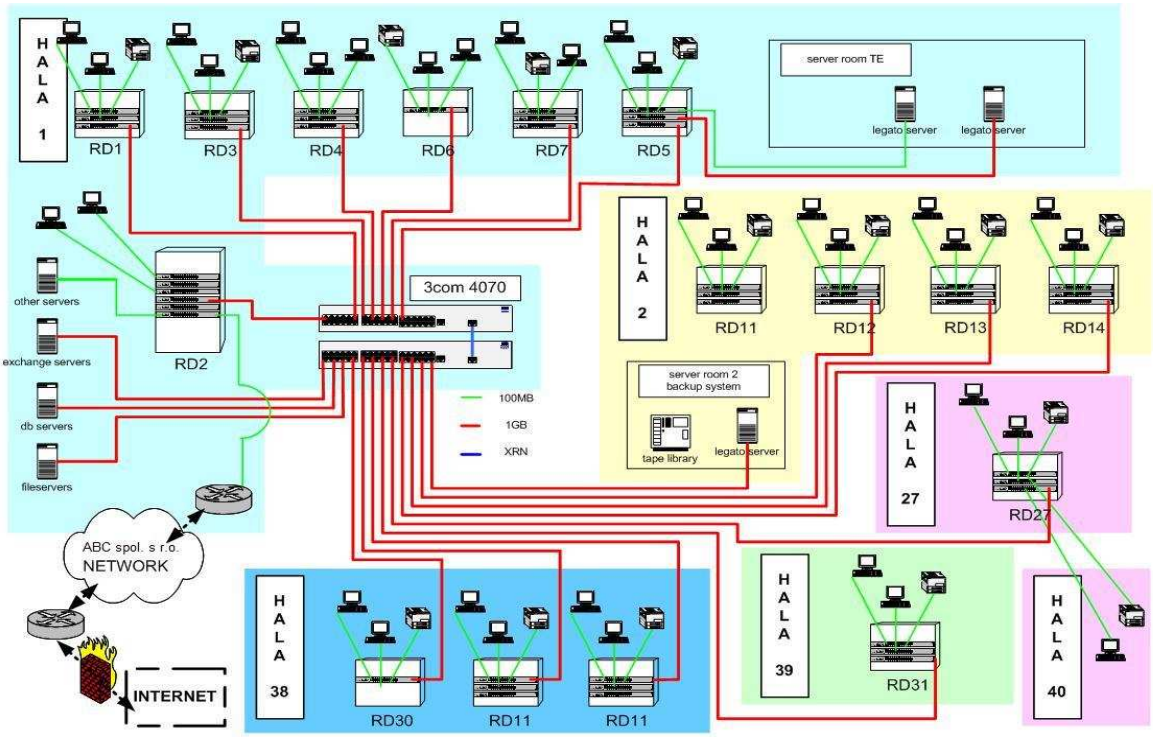
3.2 Hardwarová struktura závodu

Pobočka společnosti ABC spol. s r.o. ve Frenštátě pod Radhoštěm je vybavena veškerým klíčovým počítačovým zařízením. Pracovníci potřebující 24hodinový přístup k firemním datům jsou vybaveni podnikovými notebooky, jež se připojují vzdáleným připojením přes zabezpečenou VPN (Virtual Private Network).

Celkem se v podniku nachází:

- 90 síťových tiskáren;
- 50 lokálních tiskáren;
- 1.100 počítačových sestav a notebooků.

Na technicky náročnější projekty, jako je například instalace či úprava kabeláží a rozvodů v budovách, se najímají externí dodavatelé a pracovníci.



Obr. 3.1 Topologie sítě v závodu

3.3 Softwarová struktura závodu

Pracovní stanice THP zaměstnanců nebo vedoucích výrobních směn jsou vybaveny operačním systémem Windows XP Professional.

V loňském roce proběhl přechod kancelářského balíku Microsoft Office na verzi 2007, který je využíván jako hlavní sada programů pro úpravu textu. V základní výbavě má každý počítač nainstalován Word, Excel, Access a PowerPoint. V případě potřeby je ještě doplněn o aplikace Visio či Project.

Jako emailový klient je ve společnosti používán Lotus Notes od společnosti IBM.

Úlohu hlavního informačního systému plní SAP ve verzích R/3 a APO, které tvoří veškerou evidenci o materiálu, výrobě i výrobcích a expedici.

3.4 Klasifikace dat

Pro ochranu podnikových informací jsou vytvořeny tyto tři kategorie: veřejné, vnitřní, důvěrné. Tyto kategorie jsou popsány níže.

Centrálně stanovené šablony musí obsahovat klasifikační štítek na každé stránce, v němž se uvádí kategorie informací. Označení by mělo být viditelné na spodní straně uprostřed každé stránky.

V případě revize dokumentu je doporučeno ověřit klasifikaci, případně ji změnit odpovídajícím způsobem.

3.4.1 Veřejné

Vše co bylo výslovně schváleno oddělením marketingu a public relations k veřejnému publikování. Pro tyto dokumenty nejsou definována žádná speciální opatření.

3.4.2 Vnitřní

Základní klasifikace pro všechny dokumenty, které nejsou veřejné nebo důvěrné.

Smí být sdíleny jen mezi zaměstnanci skupiny, pro kterou jsou nezbytné k výkonu činnosti dle jejich pracovního zařazení. Třetím stranám smějí být předány jen v případě, že to je pro ABC spol. s r.o. z podnikatelského hlediska nezbytné. Elektronický přenos je povolen a šifrování není nutné. Při použití externí pošty nebo kurýra musí být informace uloženy do neprůhledné obálky nebo kontejneru. Příslušný zaměstnanec je zodpovědný za kontrolu správné adresy.

Interní informace ve fyzické formě včetně elektronických médií jako jsou USB disky, DVD a CD nesmí být ponechány bez dozoru, ledaže jsou zabezpečeny uzamčením dveří nebo uzamčením v kancelářském nábytku. Zaměstnanci pracující mimo lokalitu musí zabezpečit interní informace tak, aby nedošlo k neautorizovanému přístupu. V případě, že si zaměstnanec musí vzít interní informace mimo společnost, musí být informace po celou dobu v jeho osobním držení.

Nejsou-li informace dále použitelné, musí být roztrhány a vyhozeny do odpadu. Před vyhození úložných médií musí být všechny interní informace smazány nebo media musí být fyzicky zničena.

3.4.3 Důvěrné

Jedná se o informace, jejichž uniknutí by mohlo způsobit velkou finanční škodu nebo poškození pověsti skupiny ABC spol. s r.o.

Nesmějí být předány nikomu mimo skupinu ABC spol. s r.o. s výjimkou těch partnerů, kteří mají podepsanou dohodu o důvěrných informacích, nebo jsou požadovány zákonem. Při použití externí pošty nebo kurýra musí být informace uloženy do uzavřené obálky nebo kontejneru. Elektronickou komunikaci je možno použít jen v zašifrované podobě.

V elektronické formě smějí být informace uloženy jen zašifrované. Publikování na intranetu je povoleno jen v chráněné podobě. Vynášení důvěrných informací mimo ABC spol. s r.o. je povoleno pouze při absolutní nezbytnosti. Důvěrné informace ve všech formách nesmějí být ponechány v zavazadlech kontrolovaných na letištích (musí být

v příručním zavazadle) a nesmí být ponechány bez dozoru v hotelovém pokoji nebo v zamčeném či nezamčeném vozidle.

Při likvidaci musí být vyhozeny do speciálního kontejneru na důvěrný odpad nebo zničeny ve skartovači. Před vyhozením úložných médií musí být všechny interní informace smazány nebo media musí být fyzicky zničena. Z počítačů musí být důvěrná data smazána a musí být zabezpečena nemožnost opětného přečtení. Toto smazání dat musí být provedeno schváleným postupem podniku ABC spol. s r.o.

3.5 Uživatelské účty a řízení přístupu

Každý zaměstnanec využívající IT systémy v podniku je vlastníkem uživatelského jména (dále jen ID). ID je generován lokálním oddělením IT po obdržení požadavku na vystavení nadřízeným nového zaměstnance. Obsahuje minimálně 6 znaků, přičemž se jedná o směs písmen a číslic. Toto ID je jedinečný autorizační klíč pro všechny uživatele výpočetních systémů. S ID identifikací jsou i nastavena autorská práva uživatele do daného systému.

Autentizace jednotlivých uživatelů probíhá zadáním správné kombinace ID a hesla. Tím je především prosazena zásada důvěrnosti, ale jsou také podporovány bezpečnostní cíle celistvosti a dostupnosti.

Administrátorská práva do operačního systému a jemu podobných klíčových systémů má pouze oddělení IT. Z tohoto vyplývá, že řádoví zaměstnanci nejsou schopni instalovat na pracovní stanice dodatečný software, popřípadě provádět systémové úpravy. V případě databázových aplikací vytvořených pro lokální účely dochází k ponechání administrátorských práv vývojáři aplikace.

Zároveň se můžeme v podniku setkat i se skupinovými ID, která se používají pro přístup do systémů, které neumožňují přístup jednotlivcům nebo takto chráněná data nejsou citlivá data (tzn. nejsou z oblasti personální, účetní, financí, atp.).

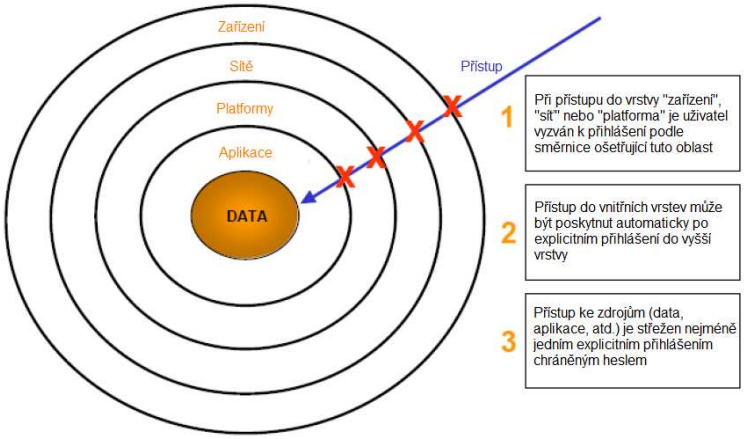
Jestliže dojde ke změně působení zaměstnance v rámci firmy nebo k ukončení pracovního vztahu, musí opět nadřízený zaměstnance vystavit požadavek na upravení přístupových práv. V případě ukončení pracovního vztahu je uživatelský účet smazán. Mění-li zaměstnanec své působiště, může si své ID ponechat a jsou mu pouze upravena práva.

3.6 Hesla

V současné době se v ABC podniku spol. s r.o. nepoužívají biometrické údaje k ověření uživatele. Zároveň v podniku není podporována technologie SSO[1].

Zaměstnancům je doporučeno vytvoření jednoho univerzálního hesla pro všechny systémy. Zaměstnanci se přihlašují pomocí hesel do těchto systémů:

- zařízení (např. PC, Notebook, Terminál, PDA, Screen Saver);
- síť (např. web, vzdálenou plochu, EDI);
- platforma (např. Windows, UNIX, OpenVMS);
- program (např. SAP R3, Mail).



Obr. 3.2 Základní uplatňovaná pravidla přístupu pomocí hesla

U nových zaměstnanců je první heslo do systému Windows a SAP generováno přímo útvarem IT. Následně je předáváno na základě ověření zaměstnance čipovou kartou s fotografií. Při prvním přihlášení do těchto systémů je každý zaměstnanec automaticky vyzván si toto automatické heslo změnit. Heslo pro emailového klienta Lotus Notes je generováno přímo programem při prvním spuštění.

Minimální délka hesla do výše uvedených systémů je nastavena na 6 znaků pro běžné uživatele a 8 znaků pro administrátory. Řetězec musí obsahovat minimálně jednu číslici a písmeno. Zároveň se znaky po sobě nesmí opakovat (např. AAAAAA, atp.). Mezery nejsou povoleny. V rámci celé společnosti ABC spol. s r.o. je definována listina tzv. černých hesel, které jsou systémově zablokovány, tím pádem je nelze uplatnit pro přístup do žádného ze systémů. Zároveň je systémově zakázáno znovu používání hesel užívaných v posledních 12 měsících.

[1]Single Sign-On - umožňuje uživateli po přihlášení do jedné aplikace automaticky přístup do všech aplikací, které jsou součástí SSO.

Platnost hesla je nastavena systémově na 90 dnů pro běžné uživatele (u administrátorů toto omezení neexistuje), po nichž je uživatel vyzván k jeho změně. V případě, že takto neučiní, je jeho účet zablokován. Pro odblokování účtu musí zaměstnanec kontaktovat oddělení IT, jež disponuje prostředky pro jeho uvolnění. Nově zvolené heslo se musí od toho minulého lišit alespoň ve 3 znacích, jinak není systémem uznáno.

Celkový počet opakovaného zadání hesla v případě překlepu nebo zapomnění je tři. Následně je uživatelský účet zablokován a je potřeba jeho obnovení za pomoci oddělení IT. Při této proceduře dochází opět k ověření uživatele.

V rámci většiny databázových aplikací vytvořených prostřednictvím MS Access není heslo po zaměstnancích vyžadováno (pouze u administrátora). Tyto systémy jsou zabezpečeny prostřednictvím seznamu uživatelů, kterým je povolen přístup. Zároveň existuje záznam o každé provedené změně v těchto systémech.

3.7 Antivirová ochrana

Každá z pracovních stanic v závodu je chráněna firewallem Windows implementovaným do operačního systému. Dále pak má každý počítač nainstalován antivirový program McAfee, který chrání data před virovými útoky.

3.8 Archivace dat

V rámci závodu stanovuje zásady pro manipulaci s dokumenty „Spisový řád“. Je vydán v souladu se zněním zákona o archivnictví a spisové službě č. 499/2004 Sb., § 8 odstavec 4.

Spisový řád se vztahuje na všechny vlastní i došlé dokumenty a je závazný pro všechny pracovníky podniku. Za jeho dodržování odpovídají jednotliví vedoucí útvarů nebo jimi pověření pracovníci a dále ostatní pracovníci v rámci své působnosti.

Spisovou službou se rozumějí práce spojené s příjmem, tříděním, doručováním, označováním, evidencí, oběhem, vyřizováním, vyhotovováním, rozmnožováním, podepisováním, odesíláním, ukládáním a vyřazováním dokumentů.

Skupina věcně totožných dokumentů tvoří jednu ukládací jednotku. Pověřený pracovník označí na obalu každé ukládací jednotky ihned při jejím založení (tj. po uložení prvního spisu) název útvaru, rok vzniku a slovní heslo, které jednoznačně vyjadřuje obsah dokumentu.

Vedoucí každého útvaru podniku i podřízené jednotky je povinen v rámci své působnosti zajistit, aby ve stanoveném termínu každého roku byly protokolárně předány

do ústřední spisovny podniku veškeré vyřízené dokumenty z uplynulého roku (po skončení operativního využití).

V současné době archivace SAP systému neprobíhá, všechna data jsou přístupná díky velikým diskovým kapacitám, které jsou podniku k dispozici.

3.9 Skartace dat

Skartační řád stanovuje a upravuje postup při vyřazování (skartaci) písemných, obrazových, zvukových či jiných záznamů v podniku. Součástí skartačního řádu je skartační rejstřík, který obsahuje seznam druhů dokumentů vyřizovaných a ukládaných v jednotlivých útvarech podniku s uvedením skartačních znaků a lhůt.

Skartační řád je závazný pro všechny pracovníky podniku. Za jeho dodržování odpovídají vedoucí jednotlivých útvarů nebo jimi pověření pracovníci a dále všichni ostatní pracovníci v rámci své působnosti. Skartační znaky a lhůty pro jednotlivé dokumenty a jejich druhy jsou uvedeny ve skartačním rejstříku. Vyskytnou-li se v podniku dokumenty, které skartační rejstřík neuvádí, posuzují se tyto ve skartačním řízení analogicky a věcně jako nejblíže příbuzné dokumenty v rejstříku uvedené.

Skartační řízení se provádí jedenkrát ročně a rozumí se jím souhrn všech pracovních úkonů prováděných při vyřazování dokumentů nadále nepotřebných pro činnost podniku.

3.10 Definice rolí a povinností v oblasti informační bezpečnosti

3.10.1 Ředitel bezpečnosti ve společnosti

V rámci ABC spol. s r.o. je jmenován takzvaný ředitel bezpečnosti (CSO - Corporate Security Officer). Součástí jeho povinností je i informační bezpečnost. CSO, jmenovaný správní radou, vlastní zodpovědnost k řešení všech konfliktů s bezpečností informací. Jako nejvýše pověřená osoba definuje bezpečnostní strategii. Vydává a dohlíží na implementaci politiky bezpečnosti, směrnic a standardů. Aktivně analyzuje aktuální bezpečnostní situaci, následně předkládá řediteli společnosti bezpečnostní rizika.

3.10.2 Manažer informační bezpečnosti

Manažer informační bezpečnosti je v rámci korporace označován zkratkou ISM (Information Security Manager). Je zodpovědný za realizaci politiky bezpečnosti informací na úrovni jednotlivých divizí společnosti. Pravidelně kontroluje a předává zprávu o stavu této politiky řediteli bezpečnosti.

3.10.3 Regionální manažer informační bezpečnosti

Regionální manažer bezpečnosti informací (RISM – Regional Information Security Manager) zajišťuje bezpečnost divizních informací a dat. Regionálně implementuje bezpečnostní standardy pro vytvoření základny k spolehlivému a důvěryhodnému obchodování v rámci regionu.

3.10.4 Lokální manažer informační bezpečnosti

Úkolem lokálního manažera informační bezpečnosti je podpora všech zaměstnanců a nadřízených v oblasti informační bezpečnosti v rámci daného závodu. Pravidelně kontroluje stav politiky bezpečnosti informací. Je zodpovědný za zpracování zprávy o stavu implementace politiky pro manažera bezpečnosti informací.

3.11 Lidské zdroje

Dle směrnice jsou všichni zaměstnanci povinni chránit informace společnosti a musí jednat v souladu se směrnicemi a postupy. Nadřízení mají povinnost prosazování informační bezpečnosti například tím, že jdou svým podřízeným příkladem v této oblasti.

Všichni zaměstnanci organizace a důležité třetí strany musí projít každý rok školením vysvětlující bezpečnostní politiku společnosti.

V případě ukončení pracovního poměru nebo ukončení spolupráce s externími subjekty musí navrátit majetek společnosti. Zároveň jsou odstraněna veškerá přístupová práva těmto osobám nebo společnostem.

3.11.1 Dohody o důvěrnosti

Tyto dohody jsou v kompetenci personálního oddělení. Směrnice ukládá každému zaměstnanci podepsat dohodu o mlčenlivosti v první pracovní den. Podepsané dohody musí být archivovány zodpovědnou osobou.

Externí partneři dostávající podniková data musí také podepsat dohodu o důvěrnosti čítající články o neodhalení a utajení před obdržením podnikových dat.

Šablona dohody je schválena právním oddělením společnosti ABC spol. s r.o. Uzavřené dohody jsou pravidelně revidovány a případně obnoveny.

3.12 Zabezpečení závodu

Ostraha je zajišťována prostřednictvím externí firmy dle pravidel a v rozsahu příslušné smlouvy o zajišťování strážní služby.

Všeobecné úkoly ostrahy:

- zabraňuje rozkrádání, zneužití, poškození nebo zničení majetku společnosti;
- zabraňuje neoprávněnému vstupu a odchodu osob nebo vjezdu a výjezdu dopravních prostředků;
- kontroluje všechny osoby a dopravní prostředky při vstupu (vjezdu) a odchodu (výjezdu);
- vede evidenci o těchto skutečnostech;
- provádí požární ochranu objektů v mimopracovní době a v době pracovního klidu;
- zachovává mlčenlivost o skutečnostech souvisejících s výkonem ostrahy společnosti.

3.13 Krizový plán

Cílem krizového plánu je chránit zdroje a pracovníky společnosti, jakož i důležité dokumenty, data a informace a docílit toho, aby rozhodující servisy v oblasti IT a zpracování dat byly vždy k dispozici.

Krizový plán z hlediska IT má vazbu na netechnickou infrastrukturu společnosti, mezi kterou řadíme správu budov, zásobování el. proudem, vodovody a kanalizace, apod. Důležitými položkami, které obsahuje, jsou:

- seznam a rozmístění serverových místností a nouzového napájení;
- topologie sítě;
- seznam všech PC, tiskáren a telekomunikačních zařízení v závodu;
- servisní smlouvy;
- pojištění.

Zároveň je důležité rozlišení:

Nouzový stav - je náhlá a neočekávaná událost, na kterou se musí bezprostředně reagovat, aby se zabránilo nebezpečí poškození, zdraví, bezpečnosti životního prostředí nebo vlastnických hodnot.

Katastrofa - je náhlá a neočekávaná událost, kterou nelze plánovat, která způsobuje obrovské poškození a ztráty. Každá událost, která znemožní celé organizaci nebo určité oblasti organizace provádění kritických hospodářských funkcí po určitou dobu. Po tuto dobu se na základě rozhodnutí vedení firmy neprovádějí běžné výrobní úkony, a pracuje se na základě firemního plánu pro řešení katastrof.

4. Příprava auditu

Společnost ABC spol. s r.o. se snaží získat pro své oddělení zabývající se podnikovou bezpečností informací InfoSec certifikaci dle normy ISO/IEC 27001:2005. Z tohoto důvodu bude práce pojednávat v části auditu v souladu s touto normou.

4.1 Cíl auditu

Cílem tohoto auditu je stanovení rozsahu splnění kritérií dle normy ISO/IEC 27001:2005 a poskytnout přehled procesů a oblastí bezpečnosti informací, které je třeba ve zkoumaném podniku inovovat.

4.2 Plán auditu

Před zahájením auditu je povinností auditora dohodnout se zadavatelem auditu jeho rozsah s ohledem na výskyt jednotlivých informačních funkcí a požadovanou (doporučenou) míru podrobnosti jejich posouzení. Audit bezpečnosti informací v této práci bude hodnotit těchto 11 základních oblastí:

Termín vykonání auditu byl stanoven na 14. 4. 2011 s tímto harmonogramem:

Čas	Článek normy		Odpovědná osoba
9:00 – 11.30	A. 5	Bezpečnostní politika.	Vedoucí útvaru IT (manažer bezpečnosti)
	A. 6	Organizace bezpečnosti informací.	
	A. 7	Řízení aktiv.	
	A. 9	Fyzická bezpečnost a bezpečnost prostředí.	
	A. 13	Řízení incidentů v oblasti bezpečnosti informací.	
	A. 14	Řízení kontinuity činností organizace.	
	A. 15	Soulad s požadavky.	
12:00 – 13:00	A. 8	Bezpečnost lidských zdrojů.	Personalistka
13:30 – 15:00	A. 10	Řízení komunikací a řízení provozu.	Vedoucí skupiny IT (Administrátor)
	A. 11	Řízení přístupu.	
	A. 12	Sběr dat, vývoj a údržba informačních systémů.	

Tabulka 4.1 Harmonogram auditu

4.3 Hodnocení auditu

V den auditu bude provedeno prošetření všech oblastí auditu. Následně obdrží každá oblast bodové ohodnocení podle toho, do jaké míry jsou jednotlivá opatření v podniku realizována. Bodové hodnocení se bude pohybovat v rozmezí 0 až 100 bodů. Přičemž 0 bodů symbolizuje stav, kdy dané opatření není v podniku vůbec zavedeno, 100 bodů pak stav zavedeného a užívaného opatření.

Práce využívá tyto stavy:

Míra plnění	Hodnocení
Opatření není zavedeno	0
Byla zavedena jen základní opatření, která jsou nevyhovující	20
Opatření je částečně splněno; podstatná část opatření není zavedena	40
Opatření je z větší části splněno	60
Opatření je převážně splněno; opatření se liší od hodnotící normy jen velmi málo	80
Opatření je zavedeno	100

Tabulka 4.2 Hodnocení jednotlivých částí auditu

Po ohodnocení každého opatření normy předloží práce míru plnění jednotlivých kapitol díky vzorci (4.1). Konečný výsledek auditu organizace předkládá ukazatel míry plnění systému řízení informační bezpečnosti (viz vzorec (4.2)).

$$MP_c{}^{1} = \frac{\text{Součet hodnocení jednotlivých opatření daného cíle}}{\text{Počet opatření daného cíle}} \times 100 \quad [\%] \quad (4.1)$$

Zdroj: PETŘÍKOVÁ, Jiřina. Audit bezpečnosti informací podle normy ISO/IEC 27001:2001: diplomová práce. Ostrava: VŠB – Technická univerzita Ostrava, Ekonomická fakulta, 2010. 79s., 2 příl.

$$MP_{ISMS}{}^{2} = \frac{\text{Součet měr plnění všech cílů ISMS}}{\text{Počet cílů v ISMS}} \quad [\%] \quad (4.2)$$

Zdroj: PETŘÍKOVÁ, Jiřina. Audit bezpečnosti informací podle normy ISO/IEC 27001:2001: diplomová práce. Ostrava: VŠB – Technická univerzita Ostrava, Ekonomická fakulta, 2010. 79s., 2 příl.

[1] MP_c je míra plnění daného cíle
[2] MP_{ISMS} je míra plnění systému řízení bezpečnosti informací

5. Provedení auditu

Tato norma obsahuje 11 oblastí bezpečnosti. Každá oblast je definována cíli a opatřeními, která by si měla prověřovaná organizace osvojit.

Cíle a jednotlivá opatření jsou citovány přímo z normy ISO/IEC 27002:2005 a jsou vyznačeny kurzívou. Práce přejala i číslování jednotlivých oblastí z normy ISO/IEC 27001:2005. V této části práce předkládá, jak výčet z normy, tak i slovní ohodnocení stavu ve zkoumané společnosti. Číselné hodnocení těchto opatření je obsaženo v tabulce (viz. Příloha 2).

A.5. Bezpečnostní politika

A.5.1 Bezpečnostní politika informací

Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení.

A.5.1.1 Dokument bezpečnostní politiky informací

Dokument bezpečnostní politiky informací musí být schválen vedoucími zaměstnanci, zveřejněn a vhodným způsobem sdělen všem zaměstnancům a příslušným externím partnerům.[8]

Společnost má zavedenu celopodnikovou bezpečnostní politiku. Jedná se o několika stránkový dokument s názvem „ABC information security policy“. Dokument byl vytvořen na základě celopodnikové analýzy bezpečnosti v souladu s normou ISO/IEC 27001:2005.

Tato politika je schválena vedením společnosti. Politika je sestavena v obecném rozsahu tak, aby vyhovovala všem závodům této společnosti. Každý závod má zavedenu individuální sestavu směrnic vycházející z této politiky, které jsou schvalovány managementem závodu.

A.5.1.2 Přezkoumání bezpečnostní politiky informací

Politika bezpečnosti musí být revidována v plánovaných intervalech nebo v případě podstatných změn pro zajištění kontinuální vhodnosti, přiměřenosti a účinnosti.[8]

Podniková bezpečnostní politika byla vytvořena v roce 2001 a od té doby nedochází k pravidelným kontrolám a změnám v dokumentu. V rámci závodu existuje směrnice „OS086 - Bezpečnost informací“ z roku 2006, která musí být revidována.

A.6. Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Řídit bezpečnost informací v organizaci.

A.6.1.1 Závazek vedení směrem k bezpečnosti informací

Vedení musí aktivně podporovat bezpečnost informací uvnitř organizace prostřednictvím jasného nasměrování, jasně vyjádřeného vlastního závazku, explicitního označení a potvrzení odpovědností za bezpečnost informací.[8]

Závazek vedení je definován v politice bezpečností informací.

A.6.1.2 Koordinace bezpečnosti informací

Aktivity pro zajištění bezpečnosti informací musí být koordinovány představiteli z různých částí organizace příslušnými úlohami v rámci systému a pracovními funkcemi.[8]

Společnost má definovánu organizační strukturu bezpečnosti informací v rámci celého koncernu. V rámci zkoumaného závodu je ředitelem jmenována osoba zodpovědná za lokální koordinaci bezpečnosti informací (vedoucí útvaru IT).

A.6.1.3 Přidělení odpovědností v oblasti bezpečnosti informací

Musí být jednoznačně vymezeny odpovědnosti za ochranu jednotlivých aktiv a za realizaci určených bezpečnostních procesů.[8]

Dle politiky nenese zodpovědnost za bezpečnost informací v závodu pouze jmenovaný řídící pracovník bezpečnosti, ale všichni vedoucí pracovníci.

A.6.1.4 Schvalovací proces prostředků pro zpracování informací

Musí být určen postup schvalování nových prostředků pro zpracování informací z pozice managementu.[8]

Postup schvalování je řešen vypsáním elektronické žádosti, která je schválena managementem po zohlednění nákladů a vhodnosti daných prostředků.

A.6.1.5 Dohody o ochraně důvěrných informací

Požadavky na důvěrnost anebo dohody o neprozrazení reflektující potřeby organizace ochránit své informace musí být identifikovány a pravidelně přezkoumány.[8]

Důvěrná data, pokud je to potřeba, jsou poskytována prostřednictvím zabezpečené VPN elektronicky a odděleně od ostatních podnikových dat. Zároveň je dohoda sestavována dle Obchodního zákoníku (513/1991 sb. §17 v platném znění). Dohody nejsou pravidelně přezkoumány.

A.6.1.6 Kontakt s autoritami

Musí být udržovány příslušné kontakty s odpovídajícími autoritami (např. s orgány státní správy).[8]

Zkoumaný závod neudržuje kontakt s autoritami ve věci bezpečnosti informací.

A.6.1.7 Kontakt se zájmovými skupinami

Musí být udržovány příslušné kontakty se zájmovými skupinami nebo speciálními fóry na bezpečnost a profesními sdruženími.[8]

Kontakt se skupinami je navázán, ale není v současné době udržován.

A.6.1.8 Nezávislé přezkoumání bezpečnosti informací

Musí být identifikována rizika, spojená s informacemi a zařízeními, fungujícími v rámci nakládání s informacemi vznikajících v procesech chodu podniku, do kterých jsou zapojeny třetí strany a přijata příslušná opatření ještě před udělením přístupových práv.[8]

Nedochází k nezávislému přezkoumání.

A.6.2 Externí partneři

Cíl: Zachovat bezpečnost zařízení pro zpracování informací a bezpečnost informačních aktiv organizace, pokud jsou přístupné třetím stranám.

A.6.2.1 Identifikace rizik vyplývající z přístupu externích partnerů

Musí být identifikována rizika, spojená s informacemi a zařízeními, fungujícími v rámci nakládání s informacemi, vznikající v procesech chodu podniku, do kterých jsou zapojeny třetí strany a přijata příslušná opatření ještě před udělením přístupových práv.[8]

Vedení závodu se snaží co nejvíce využívat vlastní zdroje technologií, které jsou u mezinárodní společnosti k dispozici. Závod ve Frenštátě pod Radhoštěm předkládá externím dodavatelům technologií požadavky na ochranu obchodního tajemství. Externí zaměstnanci podepisují dohodu o mlčenlivosti.

A.6.2.2 Zohlednění požadavků na bezpečnost informací při jednání se zákazníky

Před zpřístupněním informačních aktiv nebo informací zákazníkovi musí být zváženy všechny identifikované bezpečnostní požadavky.[8]

Závod uzavírá se zákazníky smlouvy na ochranu obchodního tajemství. Důvěrná data jsou předávána díky VPN na úložištích mimo závod.

A.6.2.3 Zohlednění požadavků na bezpečnost informací ve smlouvách s třetími stranami

Smlouvy s třetími stranami, obsahující přístupy, činnosti, komunikování nebo řízení informací organizace nebo jejího zařízení pro nakládání s informacemi, nebo doplňující produkty nebo služby k zařízením pro zpracování informací musí zohlednit všechny příslušné požadavky na bezpečnost.[8]

Závod předkládá externím třetím stranám smlouvu na ochranu obchodního tajemství a závazek mlčenlivosti. Přístup, činnosti, komunikování nebo řízení informací organizace nebo jejího zařízení pro nakládání s informacemi je prováděn až po přijetí těchto podmínek zainteresovanou třetí stranou.

A.7. Řízení aktiv

A.7.1 Odpovědnost za aktiva

Cíl: Udržovat přiměřenou ochranu aktiv organizace.

A.7.1.1 Evidence aktiv

Musí být zavedena a udržována evidence všech důležitých aktiv spojených s informačními systémy.[8]

Útvar IT si vede databázi informačních aktiv a uživatelů, kterým byla tato aktiva vydána. Zároveň disponuje seznamem SW, který je zaměstnanci využíván. Společnost si však nevede seznam datových nosičů s obchodními tajemstvími.

A.7.1.2 Vlastnictví aktiv

Všechny informace a aktiva spojená se zařízeními pro zpracování informací musí být ve vlastnictví přesně označeného útvaru organizace[8]

Ve společnosti jsou definováni vlastníci jednotlivých podnikových procesů a procedur. Výpočetní technika se stává majetkem vlastníka nebo útvaru organizace při přebírání do užívání od útvaru IT.

A.7.1.3 Přijatelné využívání aktiv

Musí být identifikována, dokumentována a zavedena pravidla pro přijatelné využívání informací a aktiv spojených se zařízeními pro zpracování informací.[8]

Je ošetřeno systémem pravidel přístupu a rolí. Částečně řeší i směrnice „OS092 - Kategorizace informací“.

A.7.2 Klasifikace informací

Cíl: Zajištění přiměřenosti ochrany informačních aktiv.

A.7.2.1 Směrnice pro klasifikaci

Informace musí být klasifikovány podle svého významu, právních požadavků, citlivosti a významnosti pro organizaci.[8]

Opatření řeší směrnice „OS092 - Kategorizace informací“, která je v současné době přepracovávána.

A.7.2.2 Označování a zpracování informací

Pro označování a zpracování informací musí být vymezen přiměřený soubor postupů, které jsou ve shodě s klasifikačním schématem přijatým organizací.[8]

Opatření řeší směrnice „OS092 - Kategorizace informací“, která je v současné době přepracovávána.

A.8. Bezpečnost lidských zdrojů

A.8.1 Před zahájením pracovního poměru

Cíl: Zajistit, aby zaměstnanci, smluvní dodavatelé a třetí strany znali své odpovědnosti a rozuměli jim a byli zároveň vhodní pro zastávání úloh v rámci systému, ke kterým byli vybráni, a tím redukovat riziko zcizení, podvodu nebo nesprávného použití zařízení.[8]

A.8.1.1 Role a odpovědnosti

Bezpečnostní úlohy a odpovědnosti zaměstnanců, smluvních dodavatelů a uživatelů z třetích stran musí být stanoveny a dokumentovány v souladu s politikou bezpečnosti informací organizace.[8]

V rámci uzavíraných smluv jsou definovány povinnosti zaměstnanců, dodavatelů a třetích stran. Zároveň zaměstnanci při podepisování smlouvy podepisují i dohody o mlčenlivosti (viz kap. 3.11.1).

A.8.1.2 Prověřování osob

Kontrola a přezkoumání předchozích činností všech kandidátů na zaměstnání, smluvních dodavatelů a uživatelů z třetích stran se musí provádět podle příslušných zákonů a pravidel a úměrně požadavkům podniku, klasifikaci informací, se kterými mají nakládat a s nimi spojených rizik.[8]

K prověřování předchozích činností kandidátů dochází spíše náhodně vedoucími pracovníky, jež pracovníky najímají na své oddělení.

A.8.1.3 Požadavky a podmínky v rámci pracovního poměru

Při uzavírání pracovní smlouvy musí zaměstnanci, smluvní dodavatelé a uživatelé z třetí strany odsouhlasit a podepsat jako součást svých podmínek pracovního poměru v pracovní smlouvě ustanovení týkající se odpovědnosti za bezpečnost informací.[8]

Zaměstnanci podepisují ustanovení až po absolvování vstupního školení zabývajícího se bezpečnosti informací.

A.8.2 V průběhu pracovního poměru

Cíl: Zajistit, aby si zaměstnanci, smluvní dodavatelé a uživatelé z třetích stran si byli vědomi bezpečnostních hrozeb a problémů, svých odpovědností a povinností, a dostatečně vybaveni, aby v průběhu své běžné práce mohli podporovat bezpečnostní politiku organizace, a aby se redukovalo riziko lidských chyb.[8]

A.8.2.1 Odpovědnost vedení

Management musí vyžadovat, aby zaměstnanci, smluvní dodavatelé a uživatelé z třetích stran dodržovali bezpečnost podle vyhlášených politik a postupů organizace.[8]

Odpovědnosti jsou definovány v pracovním řádu a ve směrnici „PIO0098 - Pořizování a používání výpočetní techniky, datové sítě a software“. Zaměstnanci mají povinnost se

seznamovat se všemi směrnicemi a dodržovat je. Vedoucím pracovníkům se navíc ukládá povinnost „jít příkladem“ svým podřízeným.

A.8.2.2 Požadavky o bezpečnosti informací, vzdělávání a výcvik

Všichni zaměstnanci organizace, a je-li to důležité, i uživatelé třetích stran musí absolvovat odpovídající, pravidelně se opakující školení vztahující se k politice bezpečnosti informací a postupům organizace.[8]

Školení jsou ve společnosti řízena a opakována v pravidelných intervalech. Školení bezpečnosti informací je prováděno každý rok vedoucími pracovníky.

A.8.2.3 Disciplinární řízení

Musí být zaveden formalizovaný disciplinární proces pro zaměstnance, kteří ohrozili bezpečnostní rozhraní.[8]

Opatření řeší pracovní řád dle zákoníku práce.

A.8.3 Ukončení nebo změna pracovního poměru

Cíl: Zajistit, aby zaměstnanci, smluvní dodavatelé a uživatelé z třetích stran opouštěli organizaci nebo měnili zaměstnání předepsaným způsobem.[8]

A.8.3.1 Odpovědnosti při ukončení pracovního poměru

Musí být jasně určeny a formulovány odpovědnosti při ukončování zaměstnaneckého poměru nebo při změně zaměstnání v rámci organizace.[8]

Opatření je řešeno výstupním listem. Postup je popsán v pracovním řádu.

A.8.3.2 Vrácení aktiv

Všichni zaměstnanci, smluvní dodavatelé a uživatelé z třetích stran musí před ukončením zaměstnání, smlouvy nebo dohody vrátit všechna aktiva, náležející organizaci, která spravovali při výkonu své funkce.[8]

Opatření je řešeno výstupním listem. Zaměstnanec dostává potvrzení o navrácení na výstupní list při vrácení každého zapůjčeného aktiva. Propouštěcí listy dostává zaměstnanec na základě vrácení všech aktiv od personálního oddělení.

A.8.3.3 Odstranění přístupových práv

Přístupová práva všech zaměstnanců, smluvních dodavatelů a uživatelů z třetích stran k informacím a zařízením pro zpracování informací musí být odejmuta před ukončením jejich zaměstnanosti, smlouvy nebo dohody nebo je změněna podle povahy změny (pokud se jedná o změnu uvnitř organizace).[8]

Odstranění přístupových práv je dle směrnice v pravomoci útvaru IT a mělo by k němu dojít do 24 hodin od podání žádosti. K odstraňování některých uživatelských účtů však do zmíněné doby nedochází.

A.9. Fyzická bezpečnost a bezpečnost prostředí

A.9.1 Zabezpečené oblasti

Cíl: Předcházet neoprávněnému přístupu, poškození a zásahům do zařízení a informací organizace. [8]

A.9.1.1 Fyzický bezpečnostní perimetr

Při ochraně prostor, ve kterých se nachází zařízení pro zpracování informací, musí organizace používat bezpečnostní perimetr (bariéry jako zdi, vstupy pomocí čipových karet, recepce apod.). [8]

Fyzický bezpečnostní perimetr je zajištěn zdmi, střeženými bránami, kamerovým systémem a přístupem s čipovými kartami.

Závod úzce sousedí s komplexem patřící jiné společnosti, která v minulosti patřila k závodu. Je stále zachován průjezd.

A.9.1.2 Opatření pro fyzický přístup osob

Bezpečné prostory musí být chráněny vhodnými opatřeními pro zajištění, aby přístup byl povolen pouze oprávněným osobám. [8]

Kontrola pohybu osob je v objektu závodu zabezpečena přístupem s čipovými kartami, kamerovým systémem a náhodnými pochůzkami ostrahy závodu. Řeší směrnice „CAP1000665 - Přidělování ID karet, docházkový a přístupový systém“.

A.9.1.3 Zabezpečení kanceláří, místností a zařízení

Pro ochranu kanceláří, místností a vybavení se zvláštními bezpečnostními požadavky musí být vytvořeny zabezpečené oblasti. [8]

Přístup do kanceláří je řešen čipovými karetami a uzamykatelností.

A.9.1.4 Ochrana proti vnějším a přírodním hrozbám

Musí být zavedena fyzická ochrana proti zničení požárem, povodní, zemětřesením, explozí, a dalším živelným nebo společenským ohrožením. [8]

Řeší havarijní plán a směrnice „Emergency plan“.

A.9.1.5 Práce v zabezpečených oblastech

Pro zvýšení bezpečnosti v zabezpečených oblastech musí být využívány další opatření a směrnice. [8]

Mezi zabezpečené oblasti jsou v závodu řazeny 2 serverové místnosti. Přístup k nim je řešen čipovými kartami, kterým musí být přidělena speciální přístupová práva.

A.9.1.6 Veřejně přístupné prostory, prostory příjmu zboží a nakládky

Přístupová místa, jako jsou např. prostory pro nakládku a vykládku a další místa, ve kterých by neautorizované osoby mohly vstoupit do organizace, musí být pod dohledem,

a pokud je to možné, izolovány od zařízení pro zpracování informací, aby nemohlo dojít k neautorizovanému přístupu. [8]

Tyto prostory jsou monitorovány především kamerovým systémem a nutností se nahlásit na vrátnici.

A.9.2 Bezpečnost zařízení

Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace. [8]

A.9.2.1 Umístění zařízení a jeho ochrana

Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí, daná prostředím a aby se omezily příležitosti pro neoprávněný přístup. [8]

Ochrana je v podniku řešena hlavně uzamykatelností kanceláří, kdy se klíče vydávají pouze vedoucím pracovníkům a čipovými kartami s přístupovými právy. Čipové karty jsou využívány velice často a dochází tak k potlačení neoprávněného přístupu.

A.9.2.2 Dodávky energie

Zařízení musí být ochráněno před selháním napájení a před dalšími formami přerušení způsobenými poruchami podpůrných zařízení. [8]

Závod disponuje záložním napájením, které umožňuje prodloužit chod zařízení o 20 minut. Zvažuje se zavedení záložního zdroje.

A.9.2.3 Bezpečnost kabeláže

Silová a telekomunikační kabeláž, která je určena pro přenos dat a podporu informačních služeb, musí být chráněna před poškozením a odposlechem. [8]

Veškerá interní kabeláž v závodu je v režii útvaru IT a je vedena skrytě.

A.9.2.4 Údržba zařízení

Aby byla zajištěna trvalá dostupnost a integrita, musí být zařízení udržována v souladu s pokyny výrobce a dokumentovanými postupy. [8]

Závod pracuje v nepřetržitém provozu. Z tohoto důvodu není prováděna kontrolní údržba a není zaznamenávána. Se zařízeními je nicméně zacházeno v souladu s pokyny výrobce a dokumentovanými postupy.

A.9.2.5 Bezpečnost zařízení vně objektu

Při ochraně zařízení, které je použito mimo objekty organizace, musí být zohledněna různá rizika prací mimo prostory organizace. [8]

Práci mimo řeší jak směrnice „OS086 - Bezpečnost informací“, tak i směrnice „PIO0098 - Pořizování a používání výpočetní techniky, datové sítě a software“. Notebooky

zatím neposkytují možnost šifrování harddisků. Přidání této možnosti bude v brzké době realizováno.

A.9.2.6 Bezpečná likvidace nebo opakované použití zařízení

Všechny prvky zařízení obsahujícího paměťové média, musí být před tím, než se dají dále k dispozici zkontrolovány, aby se zajistilo odstranění všech citlivých dat a softwarů. [8]

Opatření je řešeno smluvním partnerem pro celou společnost.

A.9.2.7 Přemístění majetku

Vybavení, informace nebo SW nesmí být přemístěny bez předchozího schválení (autorizace). [8]

Je vedena databáze všech zařízení s TCP/IP adresou. Jsou sestavena pravidla pro vydávání firemního majetku uživatelům a převod investičního majetku.

A.10. Řízení komunikací a řízení provozu

A.10.1 Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz prostředků pro zpracování informací. [8]

A.10.1.1 Dokumentace provozních postupů

Provozní postupy musí být dokumentovány, udržovány a k dispozici všem, kteří je potřebují. [8]

Provozní postupy jsou dokumentovány systémem směrnic a procedurami, které jsou dostupné všem uživatelům na interní síti.

A.10.1.2 Řízení změn

Změny na zařízeních využívaných pro práci s informacemi se musí provádět řízeným způsobem. [8]

Opatření je řešeno aplikací HelpDesk s definovanými postupy. Změna je prováděna oprávněným oddělením a řízení může tedy probíhat i na dálku. Řízené změny se konají také v systému SAP na celopodnikové úrovni.

A.10.1.3 Oddělení povinností

Povinnosti musí být odděleny od oblastí odpovědností, aby se omezila příležitost neoprávněné nebo i neúmyslné modifikace nebo zneužití aktiv organizace. [8]

V závodu jsou definovány administrátorská a uživatelská oprávnění. Změny jsou nařizovány především na celopodnikové úrovni.

A.10.1.4 Oddělení vývojového, testovacího a provozního zařízení

Vybavení pro vývoj, testování a provoz musí být od sebe odděleno, pro snížení rizika neautorizovaného přístupu nebo změn v operačním systému. [8]

Závod disponuje třemi oddělenými verzemi systému SAP: vývojový, testovací a provozní. SAP pro personální oddělení je úplně oddělen od verze pro výrobu. Vývoj databázových aplikací je řešen jednotlivými odděleními. Jiné vývojové systémy v závodu nejsou.

A.10.2 Řízení dodávek služeb třetích stran

Cíl: Zavést a udržovat přiměřenou úroveň bezpečnosti informací a dodávání služeb ve souladu s dohodami o dodání služeb třetí stranou. [8]

A.10.2.1 Dodávka služeb

Musí být zajištěno, aby smlouvy s třetí stranou o dodání služeb obsahovaly výčet bezpečnostních opatření, přesná stanovení služeb a úrovně jejich dodávání a požadavek, aby třetí strany tato ustanovení průkazně dodržovaly. [8]

Dodávky služeb jsou řešeny na bázi lokálních smluv závodu a třetí strany. Závod je schopen si většinu servisních prací obstarat sám. V případě externí spolupráce jsou přesně definovány postupy a čas oprav.

A.10.2.2 Monitorování a přezkoumávání služeb zabezpečených třetí stranou

Služby, hlášení o jejich provádění a záznamy poskytované třetí stranou, musí být pravidelně monitorovány a přezkoumány, včetně pravidelného provádění auditů. [8]

K monitorování v podniku dochází jen v případě nalezení neshody. Nejsou vytvořeny směrnice pro tuto činnost.

A.10.2.3 Řízení změn služeb poskytovaných třetími stranou

Změny v rámci poskytování služeb, včetně udržování a zlepšování existujících informačních politik, postupů a opatření, musí být řízeny. V rámci provádění změn musí být brán v úvahu význam změny ve vztahu k podnikání a jeho procesům a provedeno nové hodnocení rizik. [8]

Opatření je řešeno. Postupy nejsou zaznamenány.

A.10.3 Plánování a akceptace systému

Cíl: Minimalizovat riziko selhání systému. [8]

A.10.3.1 Kapacitní plánování

Pro zajištění požadované výkonnosti systému se musí monitorovat a vylaďovat využívání zdrojů, musí se však také dělat prognózy požadavků na budoucí kapacity. [8]

Nejsou vytvořeny procedury ošetřující toto doporučení. Počet zaměstnanců je stabilizovaný a tím i počet uživatelů, což je dostačující. Sledován je jen systém SAP z hlediska využívaných transakcí a dalších parametrů.

A.10.3.2 Akceptace systému

Musí být určena kritéria pro akceptaci nových systémů, jejich aktualizaci a zavádění nových verzí. Kritéria musí být podpořena vhodnými testy systému, které jsou prováděny před vlastní akceptací. [8]

Kritéria jsou stanovena. Jelikož se jedná o mezinárodní organizaci je toto řešeno především příkazy „shora“. Je zmíněno i v „ABC information security policy“.

A.10.4 Ochrana proti škodlivým programům a mobilním kódům

Cíl: Chránit integritu programů a dat. [8]

A.10.4.1 Opatření na ochranu proti škodlivým programům

Musí být implementována opatření pro odhalování, prevenci a znovunabytí ztracených dat, aby byla zajištěna ochrana před působením škodlivých programů a zvyšováno odpovídající bezpečnostní povědomí uživatelů. [8]

Je řešeno antivirovým systémem McAfee, který je nainstalovaný na každém PC a je automaticky aktualizován. Závod využívá firewall, který je součástí Windows XP na PC stanicích. U serveru je využíván opět McAfee.

A.10.4.2 Opatření proti mobilním kódům

Mobilní kódy nejsou ve společnosti používány.

A.10.5 Zálohování

Cíl: Chránit integritu programů a dat. [8]

A.10.5.1 Zálohování informací

Musí se pravidelně pořizovat a testovat záložní kopie informací a programového vybavení podle odsouhlasené politiky pro zálohování. [8]

V závodu dochází k zálohování každý den ve dvou variantách. Vytváří se záloha celého systému a záloha změn v systému. SAP není zálohován (viz kapitola 3.8).

A.10.6 Správa bezpečnosti sítě

Cíl: Zajistit ochranu informací v počítačových sítích a ochranu podpůrné infrastruktury. [8]

A.10.6.1 Síťová opatření

Sítě musí být přiměřeně kontrolovány a řízeny aby byly ochráněny před hrozbami a pro udržení bezpečnosti systémů a aplikací využívajících sítě, včetně přenášených informací.[8]

Přístup k síťovým složkám je řízen procedurou, na základě které je potřeba vyplnit žádost schvalovanou vedením. Sítě jsou v závodu kontrolovány a řízeny dostatečně.

A.10.6.2 Bezpečnost síťových služeb

Zvláštní požadavky na bezpečnost, úrovně služeb, a požadavky na management všech síťových služeb musí být identifikovány a zavedeny do všech smluv na síťové služby ať už jsou tyto služby poskytovány přímo na pracovišti (in-house) nebo outsourcovány. [8]

Společnost má outsourcováno internetové připojení od firmy O2. Plánuje přejít v brzké době na lokálního poskytovatele internetu a řídit si tak toto připojení samostatně. Bezpečnost je řešena kvalitním firewallem. Přístup k síti mimo závod je řešen pomocí aplikace iPass (aplikace pro bezpečné přihlášení uživatele prostřednictvím ID a hesla) a VPN vytvořením bezpečných tunelů. Připojení mimo závod je zdokumentováno v návodu, který je přístupný všem zaměstnancům.

A.10.7 Zacházení s médii

Cíl: Předcházet poškození aktiv a přerušení činnosti organizace. [8]

A.10.7.1 Správa výměnných počítačových médií

Musí existovat postupy pro správu vyměnitelných počítačových médií. [8]

Postupy existují a jsou sdělovány uživatelům ve školení „Bezpečnost informací“.

A.10.7.2 Likvidace médií

Jestliže jsou média dále provozně neupotřebitelná, musí být bezpečně a spolehlivě zlikvidována dokladovanými postupy. [8]

Opatření je řešeno. Směrnice ukládá jako zodpovědnost každému zaměstnanci bezpečně likvidovat média s informačními aktivy.

A.10.7.3 Postupy pro nakládání s informacemi

Musí být vytvořeny postupy pro nakládání s informacemi a jejich ukládání, které je chrání před neoprávněným využitím nebo prozrazením. [8]

Doporučení je řešeno ve směrnicích: „OS092 - Kategorizace informací“ a „CAP1006068 - Archivace a skartace“.

A.10.7.4 Bezpečnost systémové dokumentace

Systémová dokumentace musí být chráněna před neoprávněným přístupem. [8]

Dokumentace je uložena na síti. Je chráněna zrcadlením disku a pravidelnou archivací. Zápis do složek obsahujících systémovou dokumentaci je řešen speciálními přístupovými právy.

A.10.8 Výměny informací

Cíl: Udržovat bezpečnost informací a SW při jejich přenosu v rámci organizace i při výměnách s kteroukoliv externí organizací. [8]

A.10.8.1 Politiky a postupy výměny informací

Musí existovat politiky, postupy a opatření pro ochranu výměny informací s použitím všech typů komunikačních zařízení. [8]

Doporučení je řešeno ve směrnicích: „OS092 - Kategorizace informací“ a „OS086 - Bezpečnost informací“. Postupy jsou zaměstnancům sdělovány i na školení „Bezpečnost informací“.

A.10.8.2 Dohody o výměně informací a programů

Pro výměnu informací a SW vybavení musí mezi organizací a externími partnery být uzavřeny dohody. [8]

Ochranná opatření jsou uvedena v uzavíraných dohodách a v dodatcích o ochraně obchodního tajemství.

A.10.8.3 Bezpečnost médií při přepravě

Média obsahující informace musí být chráněna proti neautorizovanému přístupu, zneužití nebo poškození při transportu mimo organizaci. [8]

Opatření je řešeno ve směrnici „OS092 - Kategorizace informací“.

A.10.8.4 Elektronické zasílání zpráv (pošta)

Informace přenášené elektronickou poštou musí být vhodným způsobem chráněny. [8]

Opatření je řešeno ve směrnici „OS092 - Kategorizace informací“. Zaměstnanci jsou nabádáni, aby důvěrné informace šifrovali díky službě v programu Lotus Notes.

A.10.8.5 Obchodní informační systémy

Musí být vytvořeny a zavedeny politiky a postupy pro ochranu informací souvisejících s propojením obchodních IS. [8]

Opatření je řešeno ve směrnici „OS086 - Bezpečnost informací“.

A.10.9 Služby elektronického obchodu

Cíl: Zajistit bezpečnost služeb elektronického obchodu a jejich bezpečné použití. [8]

Společnost nenabízí služby elektronického obchodu.

A.10.10 Monitorováni

Cíl: Zaznamenávat neoprávněné aktivity zpracování informací. [8]

A.10.10.1 Záznamy z auditů

Auditní logy, zaznamenávající aktivity uživatelů, výjimky a události související s bezpečností informací musí být udržovány po stanovenou dobu pro účely možných budoucích vyšetřování a monitorování řízení přístupu. [8]

Opatření je řešeno. Záznamy jsou uchovávány.

A.10.10.2 Monitorování využívání systému

Musí být určeny postupy pro monitorování využití zařízení pro zpracování informací a výsledky monitorování musí být pravidelně vyhodnocovány. [8]

Vytvářejí se logy využívání systému, které se vyhodnocují. Přístup k nim má pouze vedoucí útvaru IT.

A.10.10.3 Ochrana zaznamenaných informací

Zařízení pro zaznamenávání logů musí být chráněna proti zfalšování a neoprávněnému přístupu. [8]

K záznamům mají přístup pouze administrátoři. Běžní uživatelé nemají potřebná přístupová práva.

A.10.10.4 Záznamy administrátora a operátora

Činnost administrátora a operátorů systémů se musí zaznamenávat. [8]

Záznamy jako takové jsou realizovány jen pomocí záznamů o přihlášení. Je na každém administrátorovi, zda si vede písemné záznamy o provedených činnostech.

A.10.10.5 Záznamy o chybách

Chyby se musí zaznamenávat, analyzovat a musí být přijímána příslušná opatření. [8]

Záznamy o chybách jsou automaticky nastaveny v systému SAP. Záznamy o chybách v jiných systémech a prostředích jsou zaznamenávány v aplikaci HelpDesk, kam je odesílají sami uživatelé. Analyzovány jsou pouze záznamy ze systému SAP.

A.10.10.6 Synchronizace hodin

Hodiny všech příslušných systémů zpracovávajících informace v organizaci nebo bezpečnostní zóně musí být synchronizovány podle odsouhlaseného zdroje času. [8]

Je prováděna automaticky centrálně.

A.11. Řízení přístupu

A.11.1 Požadavky podnikání

Cíl: Řídit přístup k informacím. [8]

A.11.1.1 Politika řízení přístupu

Požadavky organizace na řízení přístupu musí být vymezeny, dokumentovány a přezkoumány podle podnikových bezpečnostních požadavků na přístupy. [8]

Přístup k síťovým složkám je vydáván na základě požadavku zaměstnance přes aplikaci Share Management Tool. Tento požadavek schvaluje nadřízený zaměstnance. Přístupy k datům jsou řešeny pomocí požadavku přes aplikaci Sharepoint. Požadavky nejsou pravidelně kontrolovány.

A.11.2 Management přístupu uživatelů

Cíl: Zajistit oprávněné přístupy uživatelů a zabránit neoprávněnému přístupu do systému.[8]

A.11.2.1 Registrace uživatele

Musí existovat postup pro formální registraci uživatele včetně jejího zrušení, který zajistí propůjčení přístupu ke všem víceuživatelským informačním systémům a službám.[8]

Registrace uživatele je řešena elektronickým formulářem, který vystavuje nadřízený uživatele. Každý uživatel má své jedinečné uživatelské jméno (viz kapitola 3.5).

A.11.2.2 Řízení privilegovaného přístupu

Musí existovat systém správy a postupy pro přidělování hesel.[8]

Opatření je realizováno administrátorskými účty.

A.11.2.3 Správa hesel uživatelů

Přidělování hesel musí být řízeno formalizovaným postupem. [8]

Opatření je popsáno v politice bezpečnosti informací. Na hesla jsou kladeny speciální požadavky, které jsou vyžadovány každým systémem. Uživatelé musí svá hesla pravidelně měnit (viz kapitola 3.6).

A.11.2.4 Přezkoumání přístupových práv uživatelů

Management musí přezkoumávat v pravidelných intervalech přístupová práva uživatelů formalizovaným postupem. [8]

K přezkoumávání dochází. V systému SAP navíc dochází k vytváření X-alertů, které kontrolují kompatibilitu nastavených přístupových práv.

A.11.3 Odpovědnosti uživatelů

Cíl: Předcházet neoprávněnému přístup uživatelů. [8]

A.11.3.1 Používání hesel

Na uživatelích musí být vyžadováno, aby při výběru a použití hesel správně dodržovali bezpečnostní postupy. [8]

Uživatelská hesla se musí řídit podle pravidel stanovených v politice bezpečnosti informací a jejich dodržování je požadováno i jednotlivými systémy (viz kapitola 3.6).

A.11.3.2 Neobsluhovaná zařízení uživatelů

Na uživatelích musí být vyžadováno, aby zajistili přiměřenou ochranu neobsluhovaných zařízení. [8]

Neobsluhované PC jsou automaticky uzamčeny po systémově určené době. Uživatelé jsou ve školení „Bezpečnost informací“ vyzýváni k uzamykání svých PC po dobu nepřítomnosti a vypínání při odchodu z práce. Trvale zapnuta zůstávají pouze PC označena nálepkou „V trvalém provozu“. Vypnutí PC je kontrolováno pochůzkami ostrahy.

A.11.3.3 Politika čistého stolu a prázdné obrazovky

Musí být přijata a realizována politika čistého stolu nejen pro papíry, ale rovněž pro přenosná média a prázdné obrazovky u zařízení pro zpracování informací. [8]

Toto opatření je nařízeno a kontrolováno v rámci pravidel 5S, která jsou v závodu zavedena.

A.11.4 Řízení přístupu k síti

Cíl: Ochrana síťových služeb před neautorizovaným přístupem. [8]

A.11.4.1 Politika užívání síťových služeb

Uživatelé smí mít přímý přístup pouze ke službám, pro jejichž užití byli zvlášť oprávněni. [8]

Přístup vydává nadřízený prostřednictvím aplikace Sharepoint a Share Management Tool.

A.11.4.2 Autentizace uživatele externího připojení

Vzdálený přístup uživatelů musí být předmětem zvláštních metod autentizace. [8]

Opatření je řešeno službami iPass a VPN.

A.11.4.3 Identifikace zařízení v sítích

Jako prostředek prokázání autentického připojení ze specifických lokalit a zařízení se doporučuje využívat automatické identifikace zařízení. [8]

DHCP server využívá k autentizaci zařízení jeho IP adresu, která je svázána s MAC (fyzickou) adresou zařízení. K autentizaci dochází také díky jedinečného označení, které má přiřazeno každé PC.

A.11.4.4 Ochrana portů pro vzdálenou diagnostiku a konfiguraci

Přístup k diagnostickým portům musí být bezpečně řízen. [8]

Externí přístupy k výrobním zařízením nejsou na síti závodu. Přístup k jiným diagnostickým a konfiguračním portům je zabezpečen omezením přístupu.

A.11.4.5 Princip oddělení skupin v sítích

Do sítí musí být zavedena opatření pro oddělení skupin informačních služeb, uživatelů a IS. [8]

Dané opatření je řešeno rozdělením sítě na 104 skupin. Každá skupina má svá přístupová práva, o která musejí zaměstnanci žádat své nadřízené.

A.11.4.6 Řízení síťových spojení

Ve sdílených sítích, obzvláště v těch, které se překračují hranice organizace, musí být vymezena možnost připojení uživatelů, a to v souladu s politikou řízení přístupu (viz 11.1). [8]

Opatření je řešeno.

A.11.4.7 Řízení směrování sítě

Sdílené sítě musí být vybaveny řízeným směrováním, které zajistí, že spojení PC a informační toky nejsou v rozporu s politikou řízení přístupu k SW organizace. [8]

Opatření není řešeno.

A.11.5 Řízení přístupu k operačnímu systému

Cíl: Předcházet neautorizovanému přístupu k operačním systémům PC.[8]

A.11.5.1 Bezpečné postupy pro přihlašování

Přístup k OS musí být řízen bezpečným postupem pro přihlašování. [8]

Opatření je řešeno (viz kapitola 3.6).

A.11.5.2 Identifikace a autentizace uživatelů

Všichni uživatelé musí při své činnosti užívat jedinečný identifikátor tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti. [8]

Opatření je řešeno (viz kapitola 3.5).

A.11.5.3 Systém správy hesel

Pro zajištění efektivního a interaktivního posouzení kvality hesel musí být zaveden systém správy hesel. [8]

Opatření je řešeno.

A.11.5.4 Použití systémových nástrojů

Použití systémových programových nástrojů musí být omezeno a přísně řízeno.

Opatření je řešeno administrátorskými účty. *[8]*

A.11.5.5 Definování času odpojení stanice po nečinnosti

Neaktivní terminály na vysoce rizikových místech nebo u vysoce rizikových systémů musí být po předem určeném intervalu nečinnosti odpojeny. [8]

Opatření je realizováno uzamčením PC po systémově nastavené době.

A.11.5.6 Časové omezení spojení

Pro zajištění doplňkové bezpečnosti u vysoce rizikových aplikací musí být omezena doby, kdy je možnost se k nim připojit. [8]

Opatření není realizováno z důvodu non-stop provozu závodu.

A.11.6 Řízení přístupu k aplikacím a informacím

Cíl: Předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech. [8]

A.11.6.1 Omezení přístupu k informacím

Přístup uživatelů a podpůrných zaměstnanců k informacím a funkcím aplikačního systému musí být omezen v souladu s politikou řízení přístupu. [8]

Je řešeno řízenými přístupovými právy, která musí být udělena. Funkce jsou omezeny základní instalací. Pokud uživatel potřebuje na svém zařízení další funkce, musí o ně požádat.

A.11.6.2 Oddělení citlivých systémů

Citlivé systémy musí být provozovány v odděleném prostředí. [8]

Za citlivý se považuje systém SAP určený pro personální oddělení. Tento systém je úplně oddělen od výrobního systému.

A.11.7 Mobilní výpočetní zařízení a práce na dálku

Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a při využití prostředků pro práci na dálku. [8]

A.11.7.1 Mobilní výpočetní prostředky a komunikace

Musí existovat formální zásady a musí být schválena vhodná opatření pro ochranu před riziky, která plynou z práce na mobilních výpočetních prostředích, zejména v nechráněném prostředí. [8]

Opatření je řešeno.

A.11.7.2 Práce na dálku

Pro autorizaci a řízení práce na dálku musí být vytvořena bezpečnostní politika a postupy. [8]

Opatření je řešeno.

A.12. Sběr dat, vývoj a údržba IS

A.12.1 Požadavky na bezpečnost IS

Cíl: Zajistit, aby se bezpečnost stala nedílnou součástí informačních systémů. [8]

A.12.1.1 Analýza a specifikace požadavků na bezpečnost

Do požadavků organizace na nové IS nebo ne rozšíření existujících systémů se musí promítnout požadavky na bezpečnostní opatření. [8]

Opatření jsou prováděna na vyšších úrovních a celopodnikově.

A.12.2 Správné zpracování v aplikacích

Cíl: Předcházet ztrátě, modifikaci nebo zneužití informací v aplikačních systémech.[8]

A.12.2.1 Validace vstupních dat

Data vstupující do zpracování musí být validována, aby byla zajištěna jejich správnost a vhodnost. [8]

Opatření je ošetřeno. Data jsou kontrolována přímo systémy.

A.12.2.2 Řízení vnitřního zpracování

Pro detekci jakéhokoliv porušení informací během interního zpracování vlivem chyb při zpracování informace nebo úmyslným zásahem, musí být do aplikací začleněna validace informací. [8]

Opatření je řešeno pro systém SAP.

A.12.2.3 Integrita zpráv

Musí být identifikovány požadavky na zajištění autentičnosti a ochranu neporušenosti zpráv z aplikací a identifikována a zavedena přiměřená ochrana. [8]

Opatření je řešeno.

A.12.2.4 Validace výstupních dat

Datový výstup aplikačního systému musí být kontrolován, aby bylo zajištěno, že zpracování uložených informací probíhá správně a je přiměřené okolnostem. [8]

Opatření je řešeno pouze pro účely účetního oddělení.

A.12.3 Kryptografické prostředky

Cíl: Ochránit důvěrnost, autentičnost a integritu informací. [8]

A.12.3.1 Politika pro použití kryptografických opatření

Musí být vytvořena a dodržována příslušná politika pro použití kryptografických kontrol, které jsou určeny k ochraně informací. [8]

Kryptografická opatření jsou zohledněna v politice bezpečnosti informací jen pro emaily. Možnost kryptografie pevných disků je ve stádiu příprav.

A.12.3.2 Správa klíčů

Pro podporu kryptografických technik musí být používán systém správy klíčů, který je založen na dohodnuté soustavě norem, postupů a metod. [8]

Opatření je řešeno centrálně.

A.12.4 Bezpečnost systémových souborů

Cíl: Zajistit bezpečnost systémových souborů. [8]

A.12.4.1 Správa provozního programového vybavení

Musí existovat postupy pro řízené instalování programů do OS. [8]

Opatření je ošetřeno.

A.12.4.2 Ochrana systémových testovacích údajů

Testovací data musí být pečlivě volena, chráněna a kontrolována. [8]

Opatření není ošetřeno.

A.12.4.3 Řízení přístupu do knihovny zdrojových kódů

Přístup do knihoven zdrojových kódů programů musí být podroben přísným omezením.[8]

Opatření je ošetřeno.

A.12.5 Bezpečnost procesů vývoje a podpory

Cíl: Udržovat bezpečnost programů a informací aplikačních systémů. [8]

A.12.5.1 Postupy řízení změn

Implementace změn musí být striktně řízena s využitím postupů formálního změnového řízení. [8]

Opatření je ošetřeno ve směrnici „Change management“. SW balíky aplikací jsou řešeny centrálně pro celou společnost.

A.12.5.2 Technické přezkoumání změn operačního systému

Pokud se mění OS, musí být aplikace, významné pro podnikání přezkoumány a testovány, aby nemohlo dojít k nežádoucímu dopadu na podnikové operace nebo bezpečnost. [8]

Opatření je ošetřeno na celopodnikové úrovni.

A.12.5.3 Omezení změn programových balíků

Změny ve funkčnosti programového vybavení musí být omezeny na nezbytně nutné změny a tyto změny musí být striktně řízeny. [8]

Opatření je ošetřeno na celopodnikové úrovni.

A.12.5.4 Unik informací

Musí se předcházet možnosti úniku informací. [8]

Úniku informací se předchází poskytováním jen těch informací zaměstnancům, které nutně potřebují pro výkon své práce. Únik je ošetřen příručkou „Emergency plan“.

A.12.5.5 Programové vybavení vyvíjené externím dodavatelem

Outsourcing vývoje SW musí být pod dohledem a monitorován organizací. [8]

Opatření je ošetřeno na celopodnikové úrovni.

A.12.6 Management technické zranitelností

Cíl: Redukovat rizika pramenící z využívání publikovaných technických zranitelností.[8]

A.12.6.1 Řízení, správa a kontrola technických zranitelností

Musí se vyžadovat a získávat aktuální informace o technických zranitelnostech IS, vyhodnocovat náchylnost v rámci organizace k těmto zranitelnostem a přijímat vhodná opatření pro minimalizaci rizika. [8]

Závod si vede databázi servisů a externích partnerů. Opatření je z větší části ošetřeno celopodnikově.

A.13. Řízení incidentů v oblasti bezpečnosti informací

A.13.1 Hlášení událostí a slabých míst, týkajících se informační bezpečnosti

Cíl: Zajistit, aby byly včas komunikovány mimořádné události v rámci systému bezpečnosti informací a slabá místa spojená s IS způsobem, umožňujícím přijmout včas opatření k nápravě. [8]

A.13.1.1 Hlášení událostí týkajících se bezpečností informací

Jakmile jsou zjištěny mimořádné události v rámci systému bezpečnosti informací, musí být vhodným služebním postupem co nejdříve nahlášeny. [8]

Uživatelé mají možnost využít k takovémuto hlášení aplikaci HelpDesk. Zaměstnanci jsou k tomuto vyzýváni v politice bezpečnosti informací. Dále jsou bezpečnostní incidenty automaticky odhalovány antivirem, který posílá automatické reporty administrátorům.

A.13.1.2 Hlášení slabých míst týkajících se bezpečnosti informací

Vyžaduje se, aby všichni zaměstnanci, smluvní dodavatelé a uživatelé IS a služeb z třetích stran, zaznamenali a ohlásili jakékoliv pozorované nebo očekávané zranitelné místo v systému či hrozbu pro systém. [8]

Interní uživatelé mají možnost využít k takovémuto hlášení aplikaci HelpDesk. Zaměstnanci jsou k tomuto vyzýváni v politice bezpečnosti informací. U externích partnerů je řešeno v uzavřených smlouvách.

A.13.2 Správa informačních incidentů a zlepšení

Cíl: Zajistit, aby byl aplikován konzistentní a efektivní přístup management bezpečnostních incidentů. [8]

A.13.2.1 Odpovědnosti a postupy

Musí být stanoveny odpovědnosti managementu a postupy pro zajištění rychlé, efektivní a systematické odezvy na informaci a o bezpečnostním incidentu. [8]

Opatření je ošetřeno.

A.13.2.2 Učení se z informačních bezpečnostních incidentů

Musí být zaveden mechanismus, umožňující kvantifikovat a monitorovat druhy, rozsah, a související náklady ve vztahu vůči incidentům v rámci zajišťování bezpečnosti informací. [8]

Opatření je ošetřeno na centrální úrovni. V současné době uvažuje kancelář bezpečnosti informací nad zákazem užívání flash disků.

A.13.2.3 Shromaždování důkazů

Tam, kde dochází k následné akci proti osobám nebo organizaci po incidentu, jenž souvisí s porušením právních předpisů, musí být shromážděny důkazy a uchovány a prezentovány podle předpisů, uvedených v příslušném právním předpise. [8]

Opatření je ošetřeno na celopodnikové úrovni.

A.14. Řízení kontinuity činností organizace

A.14.1 Aspekty bezpečnosti informací při řízení kontinuity činností organizace

Cíl: Bránit přerušení činností organizace a chránit kritické postupy organizace před následky závažných chyb informačních systémů nebo havárií a zajistit jejich včasné navrácení do původního stavu. [8]

A.14.1.1 Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností

V rámci organizace musí existovat řízený proces pro rozvoj a udržování kontinuity činností organizace, který pokrývá požadavky na bezpečnost informací, nezbytné pro zachování kontinuity podnikových procesů. [8]

Opatření je ošetřeno ve směrnici „Emergency plan“.

A.14.1.2 Kontinuita činností organizace a hodnocení rizik

Musí být identifikovány události, které mohou způsobit přerušení podnikových procesů, včetně vyhodnocení pravděpodobnosti a dopadu takových přerušení a jejich důsledky na bezpečnosti informací. [8]

Opatření je prováděno celopodnikově.

A.14.1.3 Vytváření a implementace plánů kontinuity týkajících se bezpečnosti informací

Pro udržování a obnovování činností pro přerušení a zajištění dostupnosti informací musí být připraveny a zavedeny plány pro případ přerušení nebo poruchu kritických firemních aktivit. Plány musí obsahovat instrukce pro předepsané funkce včetně časové souslednosti. [8]

Opatření je prováděno celopodnikově.

A.14.1.4 Struktura plánování kontinuity

Musí být udržována jednoduchá kostra plánů kontinuity činností organizace, která zajistí, že jsou všechny plány konzistentní, konzistentně pokrývají všechny požadavky na bezpečnost, a která určí priority pro testování a údržbu. [8]

Opatření je prováděno celopodnikově. V závodu je zavedena jednoznačná organizační struktura.

A.14.1.5 Testování, udržování a přezkoumání plánů kontinuity

Plány kontinuity činnosti organizace musí být pravidelně testovány a udržovány, aby se zajistilo, že jsou aktuální a efektivní. [8]

Podle příručky „Emergency plan“ dochází k prověřování simulací nouzových stavů pravidelně.

A.15. Soulad s požadavky

A.15.1 Soulad s právními požadavky

Cíl: Vyvarovat se porušení jakýchkoliv norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků. [8]

A.15.1.1 Určení souvisejících zákonných požadavků

Pro každý IS a organizaci musí být explicitně vymezeny, dokumentovány a udržovány v aktuálním stavu požadavky, vyplývající za zákonů a ze smluv a přístup organizace, jak tyto požadavky naplnit. [8]

Opatření je řešeno. Závod vlastní certifikát ISO 9001.

A.15.1.2 Zákony na ochranu duševního vlastnictví

Musí být zavedeny příslušné postupy pro zajištění shody se zákonnými nebo smlouvami vymezenými omezeními, vztahujícími se k užití materiálů a programového vybavení, které jsou předmětem práv duševního vlastnictví. [8]

Opatření je řešeno copyrightem.

A.15.1.3 Ochrana dokladů organizace

Důležité doklady organizace musí být chráněny před ztrátou, zničením a padělám v souladu s požadavky zákonů, dalších předpisů, smluv a postupů v rámci vlastní organizace.[8]

V závodu dochází k archivaci. Přístup k archívu je omezen na 2 klíče. Jeden klíč vlastní archivářka a druhý klíč má u sebe ostraha závodu na vrátnici.

A.15.1.4 Ochrana dat a osobních údajů

Musí být zajištěna ochrana osobních údajů v souladu se zákonnými požadavky a dalšími předpisy, a pokud je to potřebné i podle požadavků ze smluv. [8]

Ochrana osobních údajů je řešena oddělením systému SAP pro personální oddělení. Kartotéky obsahující informace jsou uzamykány.

A.15.1.5 Prevence zneužití prostředků pro zpracování informací

Musí se zabránit, aby uživatelé nemohli využívat zařízení v neautorizovaném režimu.[8]

Dochází k pravidelnému: přeškolování zaměstnanců, monitorování užívání systémů a kontrolování přístupových práv.

A.15.1.6 Regulace kryptografických prostředků

Kryptografické prostředky se musí používat v souladu s dohodami, zákonnými a jinými předpisy. [8]

Opatření je řešeno jen částečně. Je řešeno pro emailovou komunikaci a u datových schránek.

A.15.2 Posouzení shody s bezpečnostními politikami a normami a technické shody

Cíl: Zajistit shodu systémů s bezpečnostními politikami organizace a normami organizace. [8]

A.15.2.1 Shoda s bezpečnostními politikami a normami

Vedoucí zaměstnanci musí zaručit, že všechny bezpečnostní postupy, které patří do jejich odpovědnosti, jsou prováděny předmětem pravidelného ověření, které posoudí soulad s bezpečnostními politikami a normami bezpečnosti. [8]

Společnost se snaží získat certifikát normy ISO/IEC 27001:2005, a proto probíhají přípravná opatření. Audity probíhají v pravidelných intervalech.

A.15.2.2 Kontrola technické shody

Musí být pravidelně ověřován soulad IS s normami pro implementaci bezpečnosti. [8]

Opatření je ošetřeno na celopodnikové úrovni. V závodu jsou IS prověřovány v rámci pravidelných auditů.

A.15.3 Aspekty auditu informačních systémů

Cíl: Maximalizovat efektivnost a minimalizovat interferenci pro provádění auditu systémů. [8]

A.15.3.1 Opatření pro audit informačních systémů

Požadavky na audit a činnosti, související s kontrolou zajištění bezpečnosti, prováděné v rámci auditu přímo na pracovních systémech se musí pečlivě plánovat a odsouhlasit v rámci organizace, aby se minimalizovalo riziko přerušení podnikových procesů. [8]

Opatření je ošetřeno na celopodnikové úrovni.

A.15.3.2 Ochrana nástrojů pro audit systému

Aby bylo zabráněno zneužití nebo ohrožení nástrojů auditu systému, musí být přístup k nim chráněn. [8]

Opatření je ošetřeno přístupovými právy.

5.1 Výsledek auditu

Dosazením do vzorce (4.2) byla vypočtena míra plnění systému řízení bezpečnosti informací. Hodnoty jsou brány z Přílohy č. 2 a jsou k vidění i v grafu 5.1. Výsledné hodnocení společnosti ABC spol. s r.o. reprezentované touto mírou je velmi dobré.

$$MP_{ISMS} = \frac{3323}{39} = \underline{\underline{85{,}2\%}}$$

Graf 5.1 Přehled míry plnění dílčích cílů ISMS (MP_c)

Zkoumaný závod společnosti ABC spol. s r.o. plánuje v brzké době obdržet certifikaci ISO/IEC 27001:2005. Vzhledem k mezinárodnímu působení podniku je bezpečnost informací

řešena celopodnikovou organizační strukturou a je řízena kanceláří vytvořenou speciálně k tomuto účelu. Bezpečnost informací je stanovena jako odpovědnost všech zaměstnanců.

Dokument bezpečnostní politiky společnosti je dostačující. Zaměstnanci jsou na tuto tématiku pravidelně proškolováni.

Lokální směrnice bohužel nebyly v minulosti pravidelně přezkoumávány. Z tohoto důvodu musí podnik:

- revidovat systém směrnic zabývající se bezpečností informací;
- stanovit pravidelný interval budoucích přezkoumání.

V rámci bezpečnosti lidských zdrojů by měl podnik zavést tato opatření:

- zlepšit systém prověřování osob před přijetím do zaměstnání;
- zaměstnancům předkládat další dohodu o mlčenlivosti při odchodu ze zaměstnání.

Z grafu 5.1 je patrné, že opatření zabývající se řízením dodávek služeb třetích stran je třeba vylepšit. Společnost se snaží veškeré služby obstarávat sama, což se díky dostupnosti finančních prostředků daří. V současné době nemá v plánu uzavřít nové smlouvy s externími dodavateli služeb. Z tohoto důvodu podniku doporučuji:

- zavést provádění náhodných kontrol dodávek stávajících služeb třetích stran.

Bodové ohodnocení opatření zabývající se zálohováním vylepší:

- zavedení kontrol zálohovacích pásek, alespoň jednou ročně, kvůli non-stop provozu závodu.

ABC spol. s r.o. plánuje v letošním roce rozšířit možnost kódování i na celé disky počítačových sestav uživatelů. Pokud společnost dodrží stejnou úroveň služby a dokumentace, která je již dnes vedena pro šifrování elektronické komunikace, pak bude toto opatření dostatečně naplněno.

Další doporučení týkající se dodržení opatření ISMS:

- vybudování náhradního zdroje elektrické energie, který je schopen pokrýt větší časové období než současný;
- zavedení administrátorského deníku nebo jiného monitorování administrátorské činnosti;
- vylepšení aplikace HelpDesk pro cílené ohlášení bezpečnostních incidentů v IS závodu;
- zlepšení komunikace se zájmovými skupinami.

6. Závěr

Řízení bezpečnosti informací ve své moderní podobě je i přes svou důležitost mladý obor. K jeho rozšíření dochází až v posledním desetiletí. Právě v mezinárodních společnostech a státní sféře je stále více prosazován, a tím jsou i vynakládány větší prostředky k ochraně informací, know-how a duševního vlastnictví. Některé součásti rodiny standardů ISO/IEC 27000 ještě nejsou kvůli rychlému pokroku v této oblasti ve své finální podobě.

Celá práce se snaží předložit cestu s cílem dosažení účinného systému řízení bezpečnosti informací. Zavedení systému řízení informační bezpečnosti představuje pro společnost výhody, jako:

- zvýšení konkurenční schopnosti;
- snížení rizik s nedostupností;
- snížení pravděpodobnosti úniku či ztráty dat;
- zlepšení prezentace organizace navenek;
- a mnoho dalších.

Společností nastavený model řízení a dodržování bezpečnosti informací je dobře zvoleným krokem. Zkoumaný závod organizace ABC spol. s r.o. dosáhl v tomto auditu velmi dobrého výsledku. Některá doporučení ještě nejsou pro dosažení certifikátu naplněna v přijatelné míře. Díky naplánované certifikaci pod zvolenou normou jsou již v podniku rozběhnuty potřebné procesy a prováděny náležité přípravy. Tímto může tato práce sloužit i jako přehled řešených částí.

Zpracování této bakalářské práce mi přiblížilo problematiku a rysy auditu jako takového. Věřím, že mé otázky a nastíněná řešení pomohou závodu úspěšně získat certifikát. Na dořešení nalezených nedostatků se bude pracovat i po odevzdání této bakalářské práce.

Seznam použité literatury

a) Knihy, příspěvky ve sborníku

[1] ARNASON, S. T., WILLETT, K. D. *How to Achieve 27001 Certification - An Example of Applied Compliance Management.* New York: Auerbach Publications, 2007. 352 s. ISBN 978-0849336485.

[2] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* 1.vyd. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

[3] DOUCEK, P., NOVÁK, L., SVATÁ, V.: *Řízení bezpečnosti informací*. 1. vyd. Praha:Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7.

[4] ERNST & YOUNG, NBÚ, DSM. *Průzkum stavu informační bezpečnosti v ČR 2009*. Praha: TATE International s.r.o., 2009. 36 s. ISBN 978-80-86813-19-6.

[5] KAFKA, Tomáš. *Průvodce pro interní audit a risk management*. 1. vydání. Praha: C.H.BECK, 2009. 192 s. ISBN 978-80-7400-121-5.

[6] KOPÁČIK, I. a kol. *Riadenie a audit v informačnej bezpečnosti.* 1. vyd. Bratislava: TATE International Slovakia, s.r.o., 2007. 322 s. ISBN 978-80-969747-0-2.

[7] SVATÁ, Vlasta. *Audit informačního systému.* 1. vyd.. Praha : Professional Publishing, 2011. 219 s. ISBN 978-80-7431-034-8.

[8] ŠEBESTA, Václav. *Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005*. Praha: Český normalizační institut, 2006. 70 s. ISBN 80-728-3204-2.

b) Elektronické publikace

[9] *eiso.cz* [online]. 2009 [cit. 2011-03-23]. E-ISO slovník. Dostupné z WWW: <http://www.eiso.cz/informacni-servis/eiso-slovnik/>.

[10] *ISO - International Organisation for Standardisation* [online]. 2009 [cit. 2011-05-01]. IT Security techniques. Dostupné z WWW: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306&published=on>.

[11] *eiso.cz* [online]. 2009 [cit. 2011-03-23]. Terminologie - Klíčová slova. Dostupné z WWW: <http://www.eiso.cz/informacni-servis/terminologie/>.

Seznam zkratek

ID	Jedinečný identifikátor uživatele
SSO	Single Sign-On
CSO	Corporate Security Officer
THP	Nevýrobní zaměstnanec
IT	Informační technologie
IS	Informační systém
PR	Public relations
VPN	Virtuální privátní síť
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
SAP	ERP systém
R/3	Distribuce systému SAP
APO	Distribuce systému SAP
PC	Počítač
H	Hodnocení
MP	Míra plnění
ISMS	Systém managementu bezpečnosti infromací
HW	Technické vybavení počítače
SW	Softwarové vybavení počítače

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);
- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 9.5.2011

Magda Vaňková

Jméno a příjmení studenta

Adresa trvalého pobytu studenta:
Podříčí 47
744 01 Frenštát pod Radhoštěm

Seznam příloh

Příloha č. 1: Černá listina hesel

Příloha č. 2: Přehled hodnocení jednotlivých opatření

Příloha č. 1: Černá listina hesel

0	1234	2222	166816
256256	1322222	7 061 992	11 111 111
19 920 706	22 222 222	!ishtar	!root
00	*111*	*12	*123
222	*23	*333*	*34
444	*45	*555*	*56
666	*67	*777*	*78
888	*89	*90	*999*
ABC	*ALLAH*	*ATE*	*AUTO*
BMW	*BOSS*	*BREMS*	*CAR*
CHEF	*COLA*	*CONTI*	*CPU*
ELA	*EMI*	*EVA*	*EVE*
GEHEIM	*HANS*	*HORST*	*HP*
HUGO	*IBM*	*INGE*	*ITT*
IXOS	*JAMES*	*JAN*	*KONI*
LISA	*LUKAS*	*MAUS*	*MAX*
MEIKE	*MOUSE*	*MTI*	*MUMMI*
NIKO	*OTTO*	*PIA*	*RAINER*
RALF	admin	ADMIN (23646)	administrator
ADOLF*	ADSM	adtran	Advance
ALAH*	ALEX*	ALFA*	alfarome
ALFRED*	ALLIN1	ALLIN1MAIL	ALLINONE
aLLy	AM	amber	AMI
AMI!SW	AMI.KEY	AMI.KEZ	AMI?SW
AMI_SW	AMI~	AMIAMI	AMIDECOD
AMIPSWD	amipswd	AMISETUP	ANDRE*
ANDREA	ANDREAS	ANDY	ANEZKA
ANGELIK	ANGELIKA	ANGIE*	anicust
ANITA*	ANJA*	ANKE*	ANNETTE
anon	ANTJE*	ANTON*	ANTONIO
ANYCOM	aPAf	apc	APPLSYS
APPS	APRIL	ARCHIVIST	ARMIN*
ARNOLD*	Asante	ascend	ASTRIT*
attack	AUGUST	autocad	Award
AWARD_SW	awkward	Babylon	BACKUP
BARBARA	BÄRBEL	BATCH	BAYER*
bbs	bciimpw	bcimpw	bcmspw
bcnaspw	BEATE*bell9	BENZ*	BERLIN
BERND*	BERTRAND	BETA*	BIANCA
BIGO	bill	bin	bintec
biodata	BIOS	BIOSPASS	biosstar
biostar	BIRGIT*	blank	bluepw
BORIS*	boss	BRAKES	BREMEN

BRENDA	BRIDGE	browsepw	BULLOCK
c	calvin	CARINA	CARMEN
CAROLA*	CAROLIAN	cc	CCC
central	CHANGE_ON_INSTALL	changeme	checkfs
checkfsys	checksys	CHEY_ARCHSVR	CHRIS*
cisco	Cisco	router	CLAUDIA
CLAUS*	CLOTH	cmaker	CNAS
COGNOS	Col2ogro2	comcomcom	Compaq
Compleri	CONCAT	condo	CONFIG (266344)
Congress	CONNIE	CONNY*	conti
CONV	CORNEEL	CORNELIA	correct
craft	craftpw	Crystal	CTX_123
CTXDEMO	CTXSYS	custpw	d.e.b.u.g
daemon	Daewuu	DANIEL*	DANIELA
DANNY*	DARLENE	DAVID*	Daytec
db2admin	dbps	DBSNMP	DCL
DEBBI*	DECEMBER	DECMAIL	DECNET
DEFAULT	default.password	Dell	DEMO
demos	DETLEF*	DETLEV	DEZEMBER
DIENSTAG	DIETER	DIETER*	DIGITAL
DISC	D-Link	dmr99	dn_04rjc
dni	DOLORIS	DONNERST	DORIS
eagle	echo	EDGAR*	EDMOND*
EDMUND	EDUARD	ELEONORA	ELEONORE
ELFI*	ELISKA	ELKE	ELKE*
ELLEN*	EMMA*	EMT*	engineer
ENGLAND	enquirypw	equalizer	ERICH*
ERNST*	ERWIN*	essex	or
ipc	extendnet	FABIAN*	fal
FAX	fax	FAXUSER	FAXWORKS
FB*	FEBRUAR	FEBRUARY	FIELD
field	FIELD.SUPPORT	FORD*	FRANCIS
FRANK*	FRANZ	FRANZ*	FRANZI*
FRAUKE	FREITAG	FRIDAY	FRIEDA
FRIEDRIC	friend	ftp	g6PJ
GABI*	GABRIELE	games	GAMMA*
GANS*	GATEWAY	GERD*	GERDA*
GERHARD	GERHART	GERRIE	GIESELA
GIESI*	GILBERT	glftpd	GOLF*
gopher	GUEST	guest1	GUESTGUE
GUESTGUEST	GUIDO*	GÜNTER	GUSTAV
h6BB	HAIKO*	halt	HAMBURG
HANA*	HANS	HANS*	HARALD
HARALD*	HARALT*	HARLEY*	HARRIS

HARRY*	HASE*	HASI*	hci
hdms	HEIDE*	HEIDI*	HEIKE
HEIKO*	HEINING	HEINRICH	HEINTZ*
HEINZ*	HELGA-S	hello	HELMUT*
HELP	HELPDESK	HERBERT	HEWITT RAND
hewlpack	HG*	HILDE*	HLT
HOLGER*	HORST	HORST*	HOST
HOUSTON	HP	HPDESK	HPLASER
HPOFFICE	HPOFFICE	DATA	HPONLY
HPP187	HPP187 SYS	HPP189	HPP196
HPWORD PUB	HU*	HUBERT	IBM
ibmcel	inads	indspw	INFO
informix	INGA*	INGEBORG	INGRES
initpw	INKA	install	Intel
INTX3	inuvik49	INVALID	iolan
IP address	ISABELLE	ISTVAN	ITALIEN
ITF3000	iwill	j09F	j256
j262	j322	j64	JAMES*
janta211	JANUAR	JANUARY	JAQUELIN
JARMILA	JDE	JENNIFER	JENS*
JOACHIM	JOLANTA	JÖRG*	JOSEF
JOSEF*	JOSEPH	JUDIT*	JULI
JULIA*	JULIE*	JULY'	JUNE
JUNI	JUTTA*	KAI*	KAISER*
KARIN*	KARL	KARMEN	KATERINA
KATHLEEN	KERSTIN	KERSTIN*	KLARA*
KLAUS*	KLEMENS	komprie	KRIS*
ksdjfg934t	l2	l3	laflaf
lantronix	LASER	LASERWRITER	last
LAURA*	LENKA*	lesarotl	letmein
LILIANE	lineprin	LINK	LKWPETER
lkwpeter	Local	User	password
locatepw	LONDON	look	looker
LORE*	LOTHAR	LOTUS	lp
lpadm	lpadmin	LR-ISDN	lucenttech1
LUCI*	lucy99	Lund	lynx
m1link	MAERZ	MAGGI*	MAI
MAIL	MAILER	maintain	maintpw
man	manager	MANAGER	Manager
MANAGER.SYS	MANFRED	MANFRED*	MANU*
MANUELA	MARCEL*	MARCH	MARCO*
MARCUS*	MAREK*	MARIA*	MARIE*
MARIO*	MARION*	MARKUS	MARLEEN
MARTA*	MARTIN	MARTINA	MÄRZ
Master	MASTER	masterkey	MATTHIAS

MAY	MBIU0	MBMANAGER	MBWATCH
mcp	MDSYS	me	MERCEDES
merlin	mfd	MGR	MGR.SYS
MICHA*	MICHAEL	MICHEL	MICHEL*
MILAN*	MITTWOCH	mMmM	MOELLER
MÖLLER*	Monday	MONI*	MONIKA
monitor	MONTAG	mountfs	mountfsys
mountsys	MPE	mpegvideo	MUCK*
MÜLLER*	MYRIAM	n/a	naadmin
NAMES	NANCY*	NAOMI*	ncadmin
ncrm	NETBASE	NetCache	NETCON
NETFRAME	NetICs	netlink	netman
NETMGR	NETNONPRIV	netopia	NETPRIV
netscreen	NetSeq	NETSERVER	NETWORK
NEWINGRES	NEWS	news	NEWYORK
NeXT	NF	NFI	NICI*
NICOL*	NINO*	nms	nmspw
NOBI*	nobody	NONPRIV	NORBERT
NOVEMBER	OCTOBER	ods	OF*
OKTOBER	OLAF*	OLIVER	OLLI*
OMNIBACK	op	OP.OPERATOR	OPEL*
OPENVIEW	OPERATOR	OPERVAX	oralcle
ORDPLUGINS	ORDSYS	OTMAR*	OUTLN
PAPER	par0t	Partner	PASCAL
PASS	PASSAT*	PASSWORD	PATRICE
PATRICK	PBX	PDP11	PDP8
PERFVIEW	permit	PETER	PETER*
PETR*	PETRA*	PHILIPPE	piranha
pixadmin	pkooltPS	PO8	Polrty
POST	Posterie	postmast	POSTMASTER
powerapp	powerdown	prime	primenet
primeos	primos	PRINT	PRINTER
PRIV	private	prost	public
pwp	q	Q54arwms	QDI
qpgmr	qsecofr	qserv	qsrv
qsrvbas	qsvr	qsysopr	quser
RADWAN	raidzone	RALF*	rcustpw
REGO	REINGARD	REMBERT	REMOTE
RENATE	RENAULT	replicator	REPORT
RICHARD	RICHART	RJE	rje
RM	RMAN	rmnetlm	ro
ROBELLE	ROBERT	rodopi	ROLAND
ROLAND*	ROMAN*	ROOT	rootpass
ROSWITHA	router	rsadmin	RSX
rw	rwa	rwmaint	SABINE

SABRE	SAHRA*	SAMSTAG	SANDRA
SANDY*	san-fran	SCHIFFER	SCHMIDT
SCHMITT	SCHUBI	SCHUMI	SCOTT*
secofr	secret	SECURITY	SEPTEMBER
SER	SERGE*	Serial Num	sertafu
SERVICE	service	setup	setup/nopassword
shutdown	SIEMENS	signa	SILKE*
SILVIA	SILVIA*	SIMON*	SIMONE
SKY_FOX	sldkj754	SnuFG5	software
SONA*	SONJA*	SONNTAG	SONY*
sp99dd	Spacve	spooml	star
start	STEEL	STEFAN	STEFAN*
STEFANIE	STEFFEN	STEFI*	STEPHEN
STUDENT	Sunday	Super	superuser
SUPERVISOR	SUPPORT	supportpw	surecom
surt	SUSANNE	SUSI*	SVEN*
SWEN*	switch	SWITCHES_SW	Sxyz
SYBILLE	SYLVIA	sync	synnet
SYS	sys	SYSADM	sysadm
sysadmin	sysbin	syslib	SYSLIB
SYSMAINT	Sysop	SYSTEM	system_admin
SYSTEST	SYSTEST_CLIG	SZYX	t0ch20x
t0ch88	TANJA*	TATIANA	TCH
tech	technolgi	tele	Telecom
TELEDEMO	TELESUP	TEST	test
teX1	TF*	TG*	THEO*
THEODOR	THOMAS	THURSDAY	TIGER
TIM*	tini	Tiny	TOBIAS
TOM*	toplayer	Toshiba	toshy99
touch	tour	TR*	tr650
TRACE	trancell	Trintech	trouble
TSEUG	TTPTHA	TUESDAY	tutor
TzqF	uClinux	UETP	ULLI*
ULRICH	ULRICH*	ULRIKE	umountfs
umountfsys	umountsys	Unix	URSULA
USER	USER_TEMPLATE	USERP	uucp
uucpadm	VACLAV	VAX	VDO
VERONIKA	VESOFT	Vextrex	VIRGINIE
VMS	VOLKER	WALTER	WALTER*
WANGTEK	web	WebBoard	webibm
weblogic	webmaster	Wednesday	welcome
WENDY*	WERNER	wg	WI*
WILLI*	WILLIAM	WINDOWS_PASST	HRU
WINSABRE	wodj	WOLF*	WOLFGANG
WONDERLAND	WOOD	WORD	www

xdfk9874t3	xljlbj	XLSERVER	xo11nE
xyzall	xyzzy	year2000	zbaaaca
Zenith	zeosx	ZUZANA	

Příloha č. 2: Přehled hodnocení jednotlivých opatření

Požadavky normy ISO/IEC 27001:2005		**H**
A. 5	Bezpečnostní politika	
A. 5.1	Bezpečnostní politika informací *Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení.*	
A. 5.1.1	Dokument bezpečnostní politiky informací	100
A. 5.1.2	Přezkoumání bezpečnostní politiky informací.	0
Míra plnění dané kapitoly		50%
A. 6	Organizace bezpečnosti informací	
A. 6.1	Interní organizace *Cíl: Řídit bezpečnost informací v organizaci.*	
A. 6.1.1	Závazek vedení směrem k bezpečnosti informací	100
A. 6.1.2	Koordinace bezpečnosti informací	100
A. 6.1.3	Přidělení odpovědností v oblasti bezpečnosti informací	100
A. 6.1.4	Schvalovací proces prostředků pro zpracování informací	100
A. 6.1.5	Dohody o ochraně důvěrných informací	100
A. 6.1.6	Kontakt s autoritami	0
A. 6.1.7	Kontakt se zájmovými skupinami	20
A. 6.1.8	Nezávislé přezkoumání bezpečnosti informací	0
Míra plnění dané kapitoly		65%
A. 6.2	Externí partneři *Cíl: Zachovat bezpečnost zařízení pro zpracování informací a bezpečnost informačních aktiv organizace, pokud jsou přístupné třetím stranám.*	
A. 6.2.1	Identifikace rizik vyplývající z přístupu externích partnerů	80
A. 6.2.2	Zohlednění požadavků na bezpečnost informací při jednání se zákazníky	100
A. 6.2.3	Zohlednění požadavků na bezpečnost informací ve smlouvách s třetími stranami	80
Míra plnění dané kapitoly		86%
A. 7	Řízení aktiv	
A. 7.1	Odpovědnost za aktiva *Cíl: Udržovat přiměřenou ochranu aktiv organizace.*	
A. 7.1.1	Evidence aktiv	80
A. 7.1.2	Vlastnictví aktiv	100
A. 7.1.3	Přijatelné využívání aktiv	100
Míra plnění dané kapitoly		93%

A. 7.2	Klasifikace informací *Cíl: Zajištění přiměřenosti ochrany informačních aktiv.*	
A. 7.1.1	Směrnice pro klasifikaci	100
A. 7.1.2	Označování a zpracování informací	100
Míra plnění dané kapitoly		100%
A. 8	Bezpečnost lidských zdrojů	
A. 8.1	Před zahájením pracovního poměru *Cíl: Zajistit, aby zaměstnanci, smluvní dodavatelé a třetí strany znali své odpovědnosti a rozuměli jim a byli zároveň vhodní pro zastávání úloh v rámci systému, ke kterým byli vybráni, a tím redukovat riziko zcizení, podvodu nebo nesprávného použití zařízení.*	
A. 8.1.1	Role a odpovědnosti	100
A. 8.1.2	Prověřování osob	40
A. 8.1.3	Požadavky a podmínky v rámci pracovního poměru	80
Míra plnění dané kapitoly		73%
A. 8.2	V průběhu pracovního poměru *Cíl: Zajistit, aby si zaměstnanci, smluvní dodavatelé a uživatelé z třetích stran si byli vědomi bezpečnostních hrozeb a problémů, svých odpovědností a povinností, a dostatečně vybaveni, aby v průběhu své běžné práce mohli podporovat bezpečnostní politiku organizace, a aby se redukovalo riziko lidských chyb.*	
A. 8.2.1	Odpovědnost vedení	100
A. 8.2.2	Požadavky o bezpečnosti informací, vzdělávání a výcvik	100
A. 8.1.3	Disciplinární řízení	80
Míra plnění dané kapitoly		93%
A. 8.3	Ukončení nebo změna pracovního poměru *Cíl: Zajistit, aby zaměstnanci, smluvní dodavatelé a uživatelé z třetích stran opouštěli organizaci nebo měnili zaměstnání předepsaným způsobem.*	
A. 8.3.1	Odpovědnosti při ukončení pracovního poměru	80
A. 8.3.2	Vrácení aktiv	100
A. 8.3.3	Odstranění přístupových práv	60
Míra plnění dané kapitoly		80%
A. 9	Fyzická bezpečnost a bezpečnost prostředí	
A. 9.1	Zabezpečené oblasti *Cíl: Předcházet neoprávněnému přístupu, poškození a zásahům do zařízení a informací organizace.*	

A. 9.1.1	Fyzický bezpečnostní perimetr	60
A. 9.1.2	Opatření pro fyzický přístup osob	100
A. 9.1.3	Zabezpečení kanceláří, místností a zařízení	100
A. 9.1.4	Ochrana proti vnějším a přírodním hrozbám	100
A. 9.1.5	Práce v zabezpečených oblastech	100
A. 9.1.6	Veřejně přístupné prostory, prostory příjmu zboží a nakládky	80
Míra plnění dané kapitoly		90%
A. 9.2	Bezpečnost zařízení *Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace.*	
A. 9.2.1	Umístění zařízení a jeho ochrana	100
A. 9.2.2	Dodávky energie	40
A. 9.2.3	Bezpečnost kabeláže	100
A. 9.2.4	Údržba zařízení	80
A. 9.2.5	Bezpečnost zařízení vně objektu	100
A. 9.2.6	Bezpečná likvidace nebo opakované použití zařízení	100
A. 9.2.7	Přemístění majetku	100
Míra plnění dané kapitoly		88%
A. 10	Řízení komunikací a řízení provozu	
A. 10.1	Provozní postupy a odpovědnosti *Cíl: Zajistit správný a bezpečný provoz prostředků pro zpracování informací.*	
A. 10.1.1	Dokumentace provozních postupů	100
A. 10.1.2	Řízení změn	100
A. 10.1.3	Oddělení povinností	80
A. 10.1.4	Oddělení vývojového, testovacího a provozního zařízení	100
Míra plnění dané kapitoly		95%
A. 10.2	Řízení dodávek služeb třetích stran *Cíl: Zavést a udržovat přiměřenou úroveň bezpečnosti informací a dodávání služeb ve souladu s dohodami o dodání služeb třetí stranou.*	
A. 10.2.1	Dodávka služeb	80
A. 10.2.2	Monitorování a přezkoumávání služeb zabezpečených třetí stranou	40
A. 10.2.3	Řízení změn služeb poskytovaných třetími stranou	80
Míra plnění dané kapitoly		66%
A. 10.3	Plánování a akceptace systému	

	Cíl: Minimalizovat riziko selhání systému.	
A. 10.3.1	Kapacitní plánování	100
A. 10.3.2	Akceptace systému	100
Míra plnění dané kapitoly		100%
A. 10.4	Ochrana proti škodlivým programům a mobilním kódům *Cíl: Chránit integritu programů a dat.*	
A. 10.4.1	Opatření na ochranu proti škodlivým programům	100
A. 10.4.2	Opatření proti mobilním kódům	100
Míra plnění dané kapitoly		100%
A. 10.5	Zálohování *Cíl: Chránit integritu programů a dat.*	
A. 10.5.1	Zálohování informací	80
Míra plnění dané kapitoly		80%
A. 10.6	Správa bezpečnosti sítě *Cíl: Zajistit ochranu informací v počítačových sítích a ochranu podpůrné infrastruktury.*	
A. 10.6.1	Síťová opatření	100
A. 10.6.2	Bezpečnost síťových služeb	100
Míra plnění dané kapitoly		100%
A. 10.7	Zacházení s médii *Cíl: Předcházet poškození aktiv a přerušení činnosti organizace.*	
A. 10.7.1	Správa výměnných počítačových médií	100
A. 10.7.2	Likvidace médií	80
A. 10.7.3	Postupy pro nakládání s informacemi	100
A. 10.7.4	Bezpečnost systémové dokumentace	100
Míra plnění dané kapitoly		90%
A. 10.8	Výměny informací *Cíl: Udržovat bezpečnost informací a SW při jejich přenosu v rámci organizace i při výměnách s kteroukoliv externí organizací.*	
A. 10.8.1	Politiky a postupy výměny informací	100
A. 10.8.2	Dohody o výměně informací a programů	100
A. 10.8.3	Bezpečnost médií při přepravě	100
A. 10.8.4	Elektronické zasílání zpráv (pošta)	100
A. 10.8.5	Obchodní informační systémy	100

Míra plnění dané kapitoly		100%
A. 10.9	Služby elektronického obchodu *Cíl: Zajistit bezpečnost služeb elektronického obchodu a jejich bezpečné použití.*	
Míra plnění dané kapitoly		0%
A. 10.10	Monitorováni *Cíl: Zaznamenávat neoprávněné aktivity zpracování informací.*	
A. 10.10.1	Záznamy z auditů	100
A. 10.10.2	Monitorování využívání systému	100
A. 10.10.3	Ochrana zaznamenaných informací	100
A. 10.10.4	Záznamy administrátora a operátora	20
A. 10.10.5	Záznamy o chybách	100
A. 10.10.6	Synchronizace hodin	100
Míra plnění dané kapitoly		87%
A. 11	Řízení přístupu	
A. 11.1	Požadavky podnikání na řízení přístupu *Cíl: Řídit přístup k informacím.*	
A. 11.1.1	Politika řízení přístupu	100
Míra plnění dané kapitoly		100%
A. 11.2	Management přístupu uživatelů *Cíl: Zajistit oprávněné přístupy uživatelů a zabránit neoprávněnému přístupu do systému.*	
A. 11.2.1	Registrace uživatele	100
A. 11.2.2	Řízení privilegovaného přístupu	80
A. 11.2.3	Správa hesel uživatelů	100
A. 11.2.4	Přezkoumání přístupových práv uživatelů	100
Míra plnění dané kapitoly		95%
A. 11.3	Odpovědnosti uživatelů *Cíl: Předcházet neoprávněnému přístup uživatelů.*	
A. 11.3.1	Používání hesel	100
A. 11.3.2	Neobsluhovaná zařízení uživatelů	80
A. 11.3.3	Politika čistého stolu a prázdné obrazovky	100
Míra plnění dané kapitoly		93%
A. 11.4	Řízení přístupu k síti *Cíl: Ochrana síťových služeb před neautorizovaným přístupem.*	

A. 11.4.1	Politika užívání síťových služeb	100
A. 11.4.2	Autentizace uživatele externího připojení	100
A. 11.4.3	Identifikace zařízení v sítích	100
A. 11.4.4	Ochrana portů pro vzdálenou diagnostiku a konfiguraci	100
A. 11.4.5	Princip oddělení skupin v sítích	100
A. 11.4.6	Řízení síťových spojení	100
A. 11.4.7	Řízení směrování sítě	0
Míra plnění dané kapitoly		86%
A. 11.5	Řízení přístupu k operačnímu systému *Cíl: Předcházet neautorizovanému přístupu k operačním systémům PC.*	
A. 11.5.1	Bezpečné postupy pro přihlašování	100
A. 11.5.2	Identifikace a autentizace uživatelů	100
A. 11.5.3	Systém správy hesel	100
A. 11.5.4	Použití systémových nástrojů	100
A. 11.5.5	Definování času odpojení stanice po nečinnosti	100
A. 11.5.6	Časové omezení spojení	0
Míra plnění dané kapitoly		83%
A. 11.6	Řízení přístupu k aplikacím a informacím *Cíl: Předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech.*	
A. 11.6.1	Omezení přístupu k informacím	100
A. 11.6.2	Oddělení citlivých systémů	100
Míra plnění dané kapitoly		100%
A. 11.7	Mobilní výpočetní zařízení a práce na dálku *Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a při využití prostředků pro práci na dálku.*	
A. 11.7.1	Mobilní výpočetní prostředky a komunikace	100
A. 11.7.2	Práce na dálku	100
Míra plnění dané kapitoly		100%
A. 12	Sběr dat, vývoj a údržba IS	
A. 12.1	Požadavky na bezpečnost IS *Cíl: Zajistit, aby se bezpečnost stala nedílnou součástí informačních systémů.*	
A. 12.1.1	Analýza a specifikace požadavků na bezpečnost	100
Míra plnění dané kapitoly		100%
A. 12.2	Správné zpracování v aplikacích	

	Cíl: Předcházet ztrátě, modifikaci nebo zneužití informací v aplikačních systémech.	
A. 12.2.1	Validace vstupních dat	100
A. 12.2.2	Řízení vnitřního zpracování	60
A. 12.2.3	Integrita zpráv	100
A. 12.2.4	Validace výstupních dat	60
Míra plnění dané kapitoly		80%
A. 12.3	Kryptografické prostředky *Cíl: Ochránit důvěrnost, autentičnost a integritu informací.*	
A. 12.3.1	Politika pro použití kryptografických opatření	40
A. 12.3.2	Správa klíčů	20
Míra plnění dané kapitoly		30%
A. 12.4	Bezpečnost systémových souborů *Cíl: Zajistit bezpečnost systémových souborů.*	
A. 12.4.1	Správa provozního programového vybavení	100
A. 12.4.2	Ochrana systémových testovacích údajů	100
A. 12.4.3	Řízení přístupu do knihovny zdrojových kódů	100
Míra plnění dané kapitoly		100%
A. 12.5	Bezpečnost procesů vývoje a podpory *Cíl: Udržovat bezpečnost programů a informací aplikačních systémů.*	
A. 12.5.1	Postupy řízení změn	100
A. 12.5.2	Technické přezkoumání změn operačního systému	100
A. 12.5.3	Omezení změn programových balíků	100
A. 12.5.4	Unik informací	100
A. 12.5.5	Programové vybavení vyvíjené externím dodavatelem	100
Míra plnění dané kapitoly		100%
A. 12.6	Management technické zranitelností *Cíl: Redukovat rizika pramenící z využívání publikovaných technických zranitelností.*	
A. 12.6.1	Řízení, správa a kontrola technických zranitelností	80
Míra plnění dané kapitoly		80%
A. 13	Řízení incidentů v oblasti bezpečnosti informací	
A. 13.1	Hlášení událostí a slabých míst, týkajících se informační bezpečnosti *Cíl: Zajistit, aby byly včas komunikovány mimořádné události v rámci systému bezpečnosti informací a slabá místa spojená s IS způsobem, umožňujícím přijmout včas opatření k nápravě.*	

A. 13.1.1	Hlášení událostí týkajících se bezpečností informací	80
A. 13.1.2	Hlášení slabých míst týkajících se bezpečnosti informací	60
Míra plnění dané kapitoly		70%
A. 13.2	Správa informačních incidentů a zlepšení *Cíl: Zajistit, aby byl aplikován konzistentní a efektivní přístup management bezpečnostních incidentů.*	
A. 13.2.1	Odpovědnosti a postupy	100
A. 13.2.2	Učení se z informačních bezpečnostních incidentů	100
A. 13.2.3	Shromaždování důkazů	100
Míra plnění dané kapitoly		100%
A. 14	Řízení kontinuity činností organizace	
A. 14.1	Aspekty bezpečnosti informací při řízení kontinuity činností organizace *Cíl: Bránit přerušení činností organizace a chránit kritické postupy organizace před následky závažných chyb informačních systémů nebo havárií a zajistit jejich včasné navrácení do původního stavu.*	
A. 14.1.1	Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností	100
A. 14.1.2	Kontinuita činností organizace a hodnocení rizik	100
A. 14.1.3	Vytváření a implementace plánů kontinuity týkajících se bezpečnosti informací	100
A. 14.1.4	Struktura plánování kontinuity	100
A. 14.1.5	Testování, udržování a přezkoumání plánů kontinuity	100
Míra plnění dané kapitoly		100%
A. 15	Soulad s požadavky	
A. 15.1	Soulad s právními požadavky *Cíl: Vyvarovat se porušení jakýchkoliv norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.*	
A. 15.1.1	Určení souvisejících zákonných požadavků	100
A. 15.1.2	Zákony na ochranu duševního vlastnictví	80
A. 15.1.3	Ochrana dokladů organizace	100
A. 15.1.4	Ochrana dat a osobních údajů	100
A. 15.1.5	Prevence zneužití prostředků pro zpracování informací	80
A. 15.1.6	Regulace kryptografických prostředků	80
Míra plnění dané kapitoly		100%
A. 15.2	Posouzení shody s bezpečnostními politikami a normami a technické shody *Cíl: Zajistit shodu systémů s bezpečnostními politikami organizace a normami organizace.*	

A. 15.2.1	Shoda s bezpečnostními politikami a normami	80
A. 15.2.2	Kontrola technické shody	80
Míra plnění dané kapitoly		80%
A. 15.3	Aspekty auditu informačních systémů *Cíl: Maximalizovat efektivnost a minimalizovat interferenci pro provádění auditu systémů.*	
A. 15.3.1	Opatření pro audit informačních systémů	100
A. 15.3.2	Ochrana nástrojů pro audit systému	80
Míra plnění dané kapitoly		90%
Míra plnění systému řízení bezpečnosti informací (ISMS)		85,2%